AirWorks AWK-3121-RTG User's Manual

Edition 4.0, October 2015

www.moxa.com/product

© 2015 Moxa Inc. All rights reserved.
Reproduction without permission is prohibited.

AirWorks AWK-3121-RTG User's Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

Copyright ©2015 Moxa Inc.
All rights reserved.
Reproduction without permission is prohibited.

Trademarks

The MOXA logo is a registered trademark of Moxa Inc.
All other trademarks or registered marks in this manual belong to their respective manufacturers.

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.

Moxa provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Technical Support Contact Information

www.moxa.com/support

Moxa Americas
Toll-free: 1-888-669-2872
Tel: +1-714-528-6777
Fax: +1-714-528-6778

Moxa China (Shanghai office)
Toll-free: 800-820-5036
Tel: +86-21-5258-9955
Fax: +86-21-5258-5505

Moxa Europe
Tel: +49-89-3 70 03 99-0
Fax: +49-89-3 70 03 99-99

Moxa Asia-Pacific
Tel: +886-2-8919-1230
Fax: +886-2-8919-1231

Table of Contents

1. Introduction 1-1
- Overview 1-2
- Package Checklist 1-2
- Product Features 1-2
- Product Specifications 1-3
- Functional Design 1-5
  - LED Indicators 1-5
  - Beeper 1-6
  - Reset Button 1-6
  - Relay (Digital Output) 1-7

2. Getting Started 2-1
- First-time Installation and Configuration 2-2
- Communication Testing 2-3
- Function Map 2-5

3. Web Console Configuration 3-1
- Web Browser Configuration 3-2
- Overview 3-3
- Basic Settings 3-4
  - System Info Settings 3-4
  - Network Settings 3-5
  - Time Settings 3-7
- Wireless Settings 3-8
  - Operation Mode 3-8
  - WLAN 3-9
  - WAC Settings 3-23
- Advanced Settings 3-23
  - VLAN Settings 3-24
  - Configuring Virtual LAN 3-25
  - DHCP Server (For AP mode only) 3-26
  - Packet Filters 3-27
  - Static Route (For Client-Router mode only) 3-29
  - NAT Settings/Port Forwarding (For Client-Router mode only) 3-30
  - SNMP Agent 3-31
  - Mobile IP Settings 3-33
- Auto Warning Settings 3-35
  - System Log 3-35
  - Syslog 3-36
  - E-mail 3-37
  - Relay 3-38
  - Trap 3-38
- Status 3-40
  - Wireless Status 3-40
  - Associated Client List (for AP mode only) 3-41
  - DHCP Client List (for AP mode only) 3-41
  - System Log 3-42
  - Relay Status 3-42
  - DI and Power Status 3-43
  - AeroLink Protection Status (For Client/Slave mode only) 3-43
  - Routing Table 3-43
  - LAN Status 3-44
- Maintenance 3-44
  - Console Settings 3-44
  - Ping 3-44
  - Firmware Upgrade 3-45
  - Config Import Export 3-45
  - Mib Export 3-46
  - Load Factory Default 3-46
  - Password 3-47
  - Locate Device 3-47
  - Misc. Settings 3-47
- Save Configuration 3-48
- Restart 3-49
- Logout 3-49

4. Software Installation and Configuration 4-1
Overview 4-2
AWK Search Utility 4-2
Installing AWK Search Utility 4-2
Configuring AWK Search Utility 4-4
5. Other Console Considerations 5-1
RS-232 Console Configuration (115200, None, 8, 1, VT100) 5-2
Configuration by Telnet and SSH Consoles 5-4
Configuration by Web Browser with HTTPS/SSL 5-5
Disabling Telnet and Browser Access 5-6
A. References A-1
Beacon A-2
DTIM A-2
Fragment A-2
RTS Threshold A-2
B. Supporting Information B-1
DoC (Declaration of Conformity) B-2
Federal Communication Commission Interference Statement B-2
R&TTE Compliance Statement B-3
Firmware Recovery B-3

1

Introduction

The AirWorks AWK-3121-RTG enables wireless users to access network resources wirelessly. The AWK-3121-RTG is rated to operate at temperatures ranging from -25 to 60°C for standard models and -40 to 75°C for wide temperature models, and is rugged enough for any harsh industrial environment.

The following topics are covered in this chapter:

- **Overview**
- **Package Checklist**
- **Product Features**
- **Product Specifications**
- **Functional Design**
  - LED Indicators
  - Beeper
  - Reset Button
  - Relay (Digital Output)

Overview

The AWK-3121-RTG access point, client, and client-router is ideal for train to ground applications. The AWK-3121-RTG can operate at temperatures ranging from -25 to 60°C for standard models and -40 to 75°C for extended temperature models, and is rugged enough for rolling stock environments. Installation is easy, with either DIN-rail mounting or wall mounting in distribution boxes. The DIN-rail/wall mounting capability, wide operating temperature range, and IP30 housing with LED indicators make the AWK-3121-RTG a convenient yet reliable solution for any wireless train to ground application.

Package Checklist

Moxa's AWK-3121-RTG is shipped with the following items. If any of these items is missing or damaged, please contact your customer service representative for assistance.

- 1 AWK-3121-RTG wireless AP/client/client-router
- 1 plastic protective cap for fiber port (AWK-3121-SSC-RTG only)
- 2 plastic RJ45 protective caps for console port
- Cable holder with 1 screw
- Quick installation guide
- Software CD
- Moxa product warranty card

NOTE Antennas are not included and must be purchased separately. The AWK is certified for use with 2 dBi omni-directional antennas with QMA to RP-SMA adapters.

Product Features

- IEEE 802.11a/b/g compliant
- Three-in-one design (AP/Client/Client-Router)
- Advanced wireless security:
  - 64-bit and 128-bit WEP/WPA/WPA2
  - SSID Hiding/IEEE 802.1X/RADIUS
  - Packet access control and filtering
- Long-distance transmission supported
- Turbo Roaming enables rapid handover (Client / Client-Router mode)
- Moxa's 50 ms Turbo Roaming technology enables seamless handover (must be used with the WAC-1001, WAC-2004, and RTG/TAP models)
- ABC-01 for configuration import/export
- Dedicated antenna selection
- Free firmware update for more advanced functions
- RS-232 console management
- 2 DIs + 1 DO for on-site monitoring and warnings
- Wide -40 to 75°C operating temperature range (T models)
- Redundant 24 VDC power inputs or IEEE 802.3af power-over-Ethernet
- DIN rail or wall mounting
- IP30 protected high-strength metal housing

Product Specifications

WLAN Interface

Standards:

IEEE 802.11a/b/g for Wireless LAN
IEEE 802.11i for Wireless Security
IEEE 802.3 for 10BaseT
IEEE 802.3u for 100BaseTX
IEEE 802.3af for Power-over-Ethernet

Spread Spectrum and Modulation (typical):

• DSSS with DBPSK, DQPSK, CCK
• OFDM with BPSK, QPSK, 16QAM, 64QAM
• 802.11b: CCK @ 11/5.5 Mbps, DQPSK @ 2 Mbps, DBPSK @ 11 Mbps
• 802.11a/g: 64QAM @ 54/48 Mbps, 16QAM @ 36/24 Mbps, QPSK @ 18/12 Mbps, BPSK @ 9/6 Mbps

Operating Channels (central frequency):

US:
2.412 to 2.462 GHz (11 channels)
5.18 to 5.24 GHz (4 channels)
5.26 to 5.825 GHz (optional)
EU:
2.412 to 2.472 GHz (13 channels)
5.18 to 5.24 GHz (4 channels)
5.26 to 5.825 GHz (optional)
*Special band such as 5.9GHz is customizable.

Security:

• SSID broadcast enable/disable
• Firewall for MAC/IP/Protocol/Port-based filtering
• 64-bit and 128-bit WEP encryption, WPA /WPA2-Personal and Enterprise (IEEE 802.1X/RADIUS, TKIP and AES)

Transmission Rates:

802.11b: 1, 2, 5.5, 11 Mbps
802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps

TX Transmit Power:

AWK-3121-M12-RTG and AWK-3121-SSC-RTG:
802.11b:
Typ. 23±1.5 dBm @ 1 to 11 Mbps
802.11g:
Typ. 20±1.5 dBm @ 6 to 24 Mbps, Typ. 19±1.5 dBm @ 36 Mbps, Typ. 18±1.5 dBm @ 48 Mbps, Typ. 17±1.5 dBm @ 54 Mbps
802.11a:
Typ. 18±1.5 dBm @ 6 to 24 Mbps, Typ. 16±1.5 dBm @ 36 to 48 Mbps, Typ. 15±1.5 dBm @ 54 Mbps
AWK-3121-M12-HP-RTG:
802.11b:
Typ. 26±1.5 dBm @ 1 to 11 Mbps
802.11g:
Typ. 26±1.5 dBm @ 6 to 24 Mbps, Typ. 25±1.5 dBm @ 36 Mbps, Typ. 24±1.5 dBm @ 48 Mbps, Typ. 23±1.5 dBm @ 54 Mbps
802.11a:
Typ. 26±1.5 dBm @ 6 to 24 Mbps, Typ. 25±1.5 dBm @ 36 Mbps, Typ. 24±1.5 dBm @ 48 Mbps, Typ. 23±1.5 dBm @ 54 Mbps

RX Sensitivity:
802.11b:
-97 dBm @ 1 Mbps, -94 dBm @ 2 Mbps, -92 dBm @ 5.5 Mbps, -90 dBm @ 11 Mbps
802.11g:
-93 dBm @ 6 Mbps, -91 dBm @ 9 Mbps, -90 dBm @ 12 Mbps, -88 dBm @ 18 Mbps, -84 dBm @ 24 Mbps, -80 dBm @ 36 Mbps, -76 dBm @ 48 Mbps, -74 dBm @ 54 Mbps
802.11a:
-90 dBm @ 6 Mbps, -89 dBm @ 9 Mbps, -89 dBm @ 12 Mbps, -85 dBm @ 18 Mbps, -83 dBm @ 24 Mbps, -79 dBm @ 36 Mbps, -75 dBm @ 48 Mbps, -74 dBm @ 54 Mbps

Protocol Support

General Protocols: Proxy ARP, DNS, HTTP, HTTPS, IP, ICMP, SNTP, TCP, UDP, RADIUS, SNMP, PPPoE, DHCP
AP-only Protocols: ARP, BOOTP, DHCP, dynamic VLAN-Tags for 802.1X-Clients

Interface

Default Antennas*:
2 dual-band omni-directional antennas, 2 dBi, RP-SMA (male)
*Only available with the AWK-3121-SSC-RTG models.
Connector for External Antennas:
AWK-3121-SSC-RTG: RP-SMA (female)
AWK-3121-M12-RTG and AWK-3121-M12-HP-RTG: QMA (female)
Fiber Ports: 1, 100BaseFX port (SC connector, AWK-3121-SSC-RTG only)
M12 Ports: 1, 10/100BaseT(X) auto negotiation speed, F/H duplex mode, and auto MDI/MDI-X connection (AWK-3121-M12-RTG and AWK-3121-M12-HP-RTG only)
Console Port: RS-232 (RJ45-type)
LED Indicators: PWR1, PWR2, PoE*, FAULT, STATE, signal strength, CLIENT MODE, WLAN, 10/100 (M12 port), 100M (fiber port)
*PoE is only available for the AWK-3121-M12-RTG and AWK-3121-M12-HP-RTG
Alarm Contact: 1 relay output with current carrying capacity of 1 A @ 24 VDC
Digital Inputs: 2 electrically isolated inputs
• +13 to +30 V for state "1"
• +3 to -30 V for state "0"
• Max. input current: 8 mA

Optical Fiber*

	100BaseFX
	Single Mode
Wavelength	1310 nm
Max. TX	0 dBm
Min. TX	-5 dBm
RX Sensitivity	-34 dBm
Link Budget	29 dB
Typical Distance	40 km
Saturation	-3 dBm

*Only available for AWK-3121-SSC models

Physical Characteristics

Housing: Metal, providing IP30 protection
Weight: 850 g
Dimensions: 53.6 x 135 x 105 mm (2.11 x 5.31 x 4.13 in)
Installation: DIN-Rail mounting, wall mounting (with optional kit)

Environmental Limits

Operating Temperature:
Standard Models: -25 to 60°C (-13 to 140°F)
Wide Temp. Models: -40 to 75°C (-40 to 167°F)
Storage Temperature: -40 to 85°C (-40 to 185°F)
Ambient Relative Humidity: 5% to 95% (non-condensing)

Power Requirements

Input Voltage: 12 to 48 VDC, redundant dual DC power inputs or 48 VDC Power-over-Ethernet (IEEE 802.3af compliant)*

*Compliant with EN 50155 on 24 VDC

Connector: 10-pin removable terminal block

Power Consumption:

12 to 48 VDC, 0.121 to 0.494 A (max.)

AWK-3121-M12-RTG: Maximum 7.9 watts

AWK-3121-M12-HP-RTG: Maximum 7.9 watts

AWK-3121-SSC-RTG: Maximum 8.1 watts

Reverse Polarity Protection: Present

Standards and Certifications

Safety: UL 60950-1, EN 60950-1

EMC: EN 301 489-1/17; FCC Part 15, Subpart B; EN 55022/55024

Radio: EN 300 328, EN 301 893

Rail Traffic: EN 50155*, EN 50121-1/4

*Complies with a portion of EN 50155 specifications. Please contact Moxa or a Moxa distributor for details.

Reliability

MTBF (mean time between failures):

AWK-3121-M12-RTG: 480,831 hrs

AWK-3121-M12-HP-RTG: 447,861 hrs

AWK-3121-SSC-RTG: 445,913 hrs

Warranty

Warranty Period: 5 years

Details: See www.moxa.com/warranty

ATTENTION

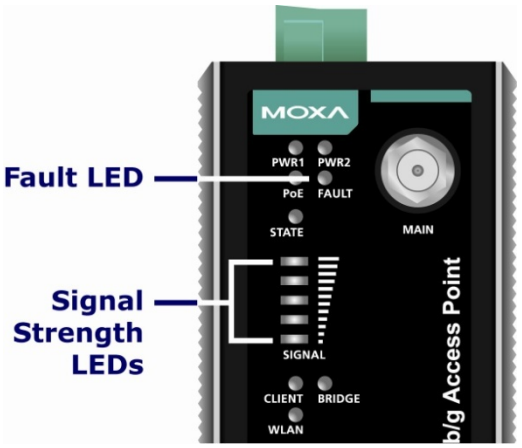
- The AWK-3121-RTG is NOT a portable mobile device and should be located at least 20 cm away from the human body.
- The AWK-3121-RTG is NOT designed for the general public. A well-trained technician should be enlisted to ensure safe deployment of AWK-3121-RTG units, and to establish a wireless network.

Functional Design

LED Indicators

The LEDs on the front panel of the AWK-3121-RTG provide a quick and easy means of determining the current operational status and wireless settings.

The **FAULT** LED indicates system failures and user-configured events. If the AWK-3121-RTG cannot retrieve the IP address from a DHCP server, the **FAULT** LED will blink at one second intervals. The **SIGNAL** LEDs indicate signal strength, and only operate in **Client/Client-Router** mode.



The following table summarizes how to read the device's wireless settings from the LED displays. More information is available in Chapter 3 in the "Basic Wireless Settings" section.

Basic Wireless Settings	LEDs			Note
Operation mode	**CLIENT**	**BRIDGE**	**SIGNAL**	
AP	off	off	–	AP mode
Client/Client-Router	on	off	0	Client mode: no association
Client/Client-Router	on	off	1	Client mode: associated, poor signal
Client/Client-Router	on	off	2-5	Client mode: associated, good signal

NOTE The current firmware version of the AWK-3121-RTG does not support Bridge, and consequently the BRIDGE LED is not functional.

ATTENTION

If the **FAULT**, **SIGNAL**, **CLIENT**, and **WLAN** LEDs light up simultaneously and blink at one-second intervals, then the system has failed to boot up. This may be due to improper operation or factors beyond your control, such as an unexpected shutdown during a firmware update. Instructions on how to recover the firmware can be found in Chapter 6 in the "Firmware Recovery" section.

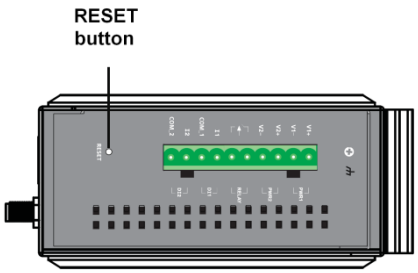
Beeper

The beeper emits two short beeps when the system is ready.

Reset Button

The **RESET** button is located on the top panel of the AWK-3121-RTG. You can reboot the AWK-3121-RTG or reset it to factory default settings by pressing the **RESET** button with a pointed object such as an unfolded paper clip.

- **System reboot:** Hold the RESET button down for under 5 seconds and then release.
- **Reset to factory default:** Hold the RESET button down for *over* 5 seconds until the **STATE** LED starts blinking green. Release the button to reset the AWK-3121-RTG.



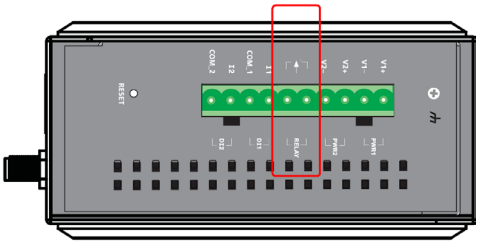
Relay (Digital Output)

The AWK-3121-RTG has one relay output consisting of the 2 terminal block contacts on the top panel, as shown below. These relay contacts are used to forward system failures and user-configured events.

The 2 wires attached to the relay contacts form an open circuit when a user-configured event is triggered. If a user-configured event does not occur, the relay circuit will remain closed. For safety reasons, the relay circuit is kept open when the AWK-3121-RTG is not powered up.

Summary of the AWK-3121-RTG's Relay Status

Power Status	Event	Relay
Off	–	Open
On	Yes	Open
	No	Short



2

Getting Started

In this chapter, we explain how to install Moxa's AirWorks AWK-3121-RTG for the first time, and quickly set up your wireless network and test whether the connection is running well. The function guide provides a convenient means of determining which functions you need to use.

The following topics are covered in this chapter:

- **First-time Installation and Configuration**
- **Communication Testing**
- **Function Map**

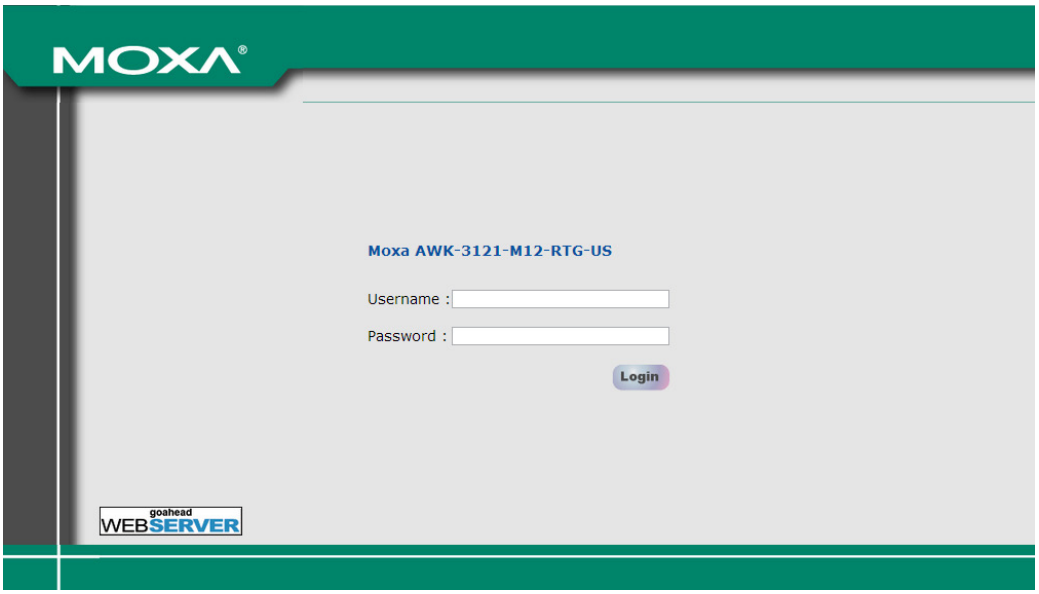
First-time Installation and Configuration

Before installing the AWK-3121-RTG, make sure that all items in the Package Checklist are in the box. You will need access to a notebook computer or PC equipped with an Ethernet port. The AWK-3121-RTG has a default IP address that must be used when connecting to the device for the first time.

- **Step 1: Select the power source.**
  The AWK-3121-RTG can be powered by a DC power input or PoE (Power over Ethernet). The AWK-3121-RTG will use whichever power source you choose.
- **Step 2: Connect the AWK-3121-RTG to a notebook or PC.**
  Since the AWK-3121-RTG supports MDI/MDI-X auto-sensing, you can use either a straight-through cable or crossover cable to connect the AWK-3121-RTG to a computer. The LED indicator on the AWK-3121-RTG's LAN port will light up when a connection is established.
- **Step 3: Set up the computer's IP address.**
  Choose an IP address on the same subnet as the AWK-3121-RTG. Since the AWK-3121-RTG's default IP address is **192.168.127.253**, and the subnet mask is **255.255.255.0**, you should set the IP address of the computer to **192.168.127.xxx**.

NOTE After you select **Maintenance** → **Load Factory Default** and click the **Submit** button, the AWK-3121-RTG will be reset to factory default settings and the IP address will be reset to **192.168.127.253**.

- **Step 4: Use the web-based manager to configure the AWK-3121-RTG**
  Open your computer's web browser and type **http://192.168.127.253** in the address field to access the homepage of the web-based Network Manager. Before the homepage opens, you will need to enter the user name and password as shown in the following figure. For first-time configuration, enter the default user name and password and then click on the **Login** button:

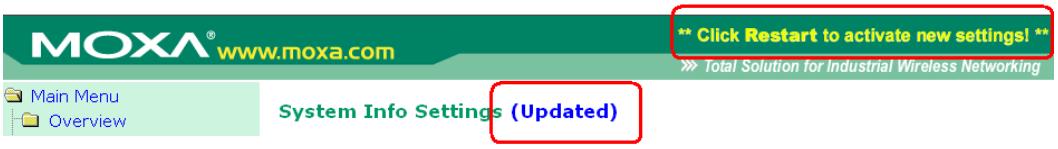


NOTE Default user name and password:

User Name: **admin**
Password: **root**

For security reasons, we strongly recommend changing the default password. To do so, select **Maintenance** → **Password**, and then follow the on-screen instructions to change the password.

NOTE After you click **Submit** to apply changes the web page will refresh, and **(Updated)** will appear on the page and a blinking reminder will be shown on the upper-right corner of the web page:



To activate the changes click **Restart** and then **Save and Restart** after you change the settings. About 30 seconds are needed for the AWK-3121-RTG to complete the reboot procedure.

- **Step 5: Select the AWK-3121-RTG operation mode.**
  By default, the AWK-3121-RTG's operation mode is set to AP. You can change to Client mode in **Wireless Settings → Basic Wireless Settings**. Detailed information about configuring the AWK-3121-RTG's operation can be found in Chapter 3.
- **Step 6: Test communications.**
  In the following sections we describe two test methods that can be used to ensure that a network connection has been established.

Communication Testing

After installing the AWK-3121-RTG you can run a sample test to make sure the AWK-3121-RTG and wireless connection are functioning normally. Two testing methods are described below. Use the first method if you are using only one AWK-3121-RTG device, and use the second method if you are using two or more AWK-3121-RTG units.

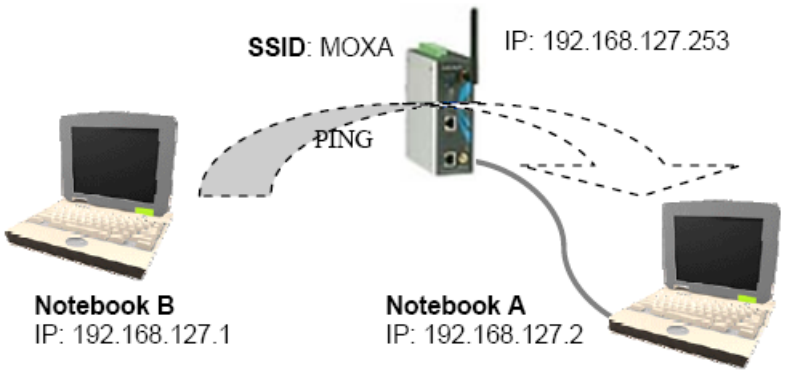
How to Test One AWK-3121-RTG

If you are only using one AWK-3121-RTG, you will need a second notebook computer equipped with a WLAN card. Configure the WLAN card to connect to the AWK-3121-RTG (NOTE: the default SSID is **MOXA**), and change the IP address of the second notebook (Notebook B) so that it is on the same subnet as the first notebook (Notebook A), which is connected to the AWK-3121-RTG.

After configuring the WLAN card, establish a wireless connection with the AWK-3121-RTG and open a DOS window on Notebook B. At the prompt, type

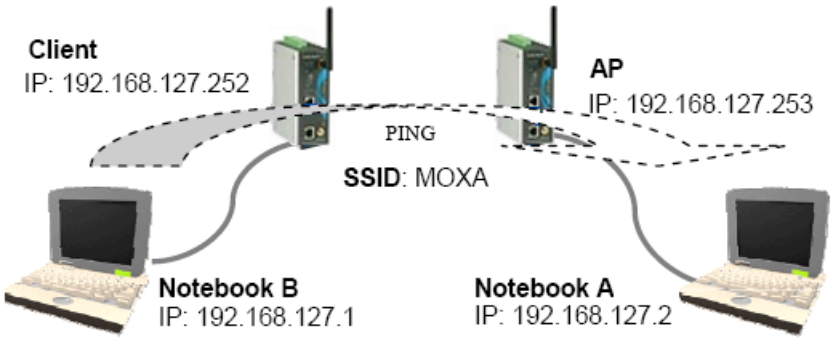
ping *<IP address of notebook A>*

and then press **Enter** (see the figure below). A "Reply from IP address …" response means the communication was successful. A "Request timed out." response means the communication failed. In this case, recheck the configuration to make sure the connections are correct.



How to Test Two or More AWK-3121-RTG Units

If you have two or more AWK-3121-RTG units, you will need a second notebook computer (Notebook B) equipped with an Ethernet port. Use the default settings for the first AWK-3121-RTG connected to notebook A and change the second or third AWK-3121-RTG connected to notebook B to Client mode, and then configure the notebooks and AWK-3121-RTG units properly.

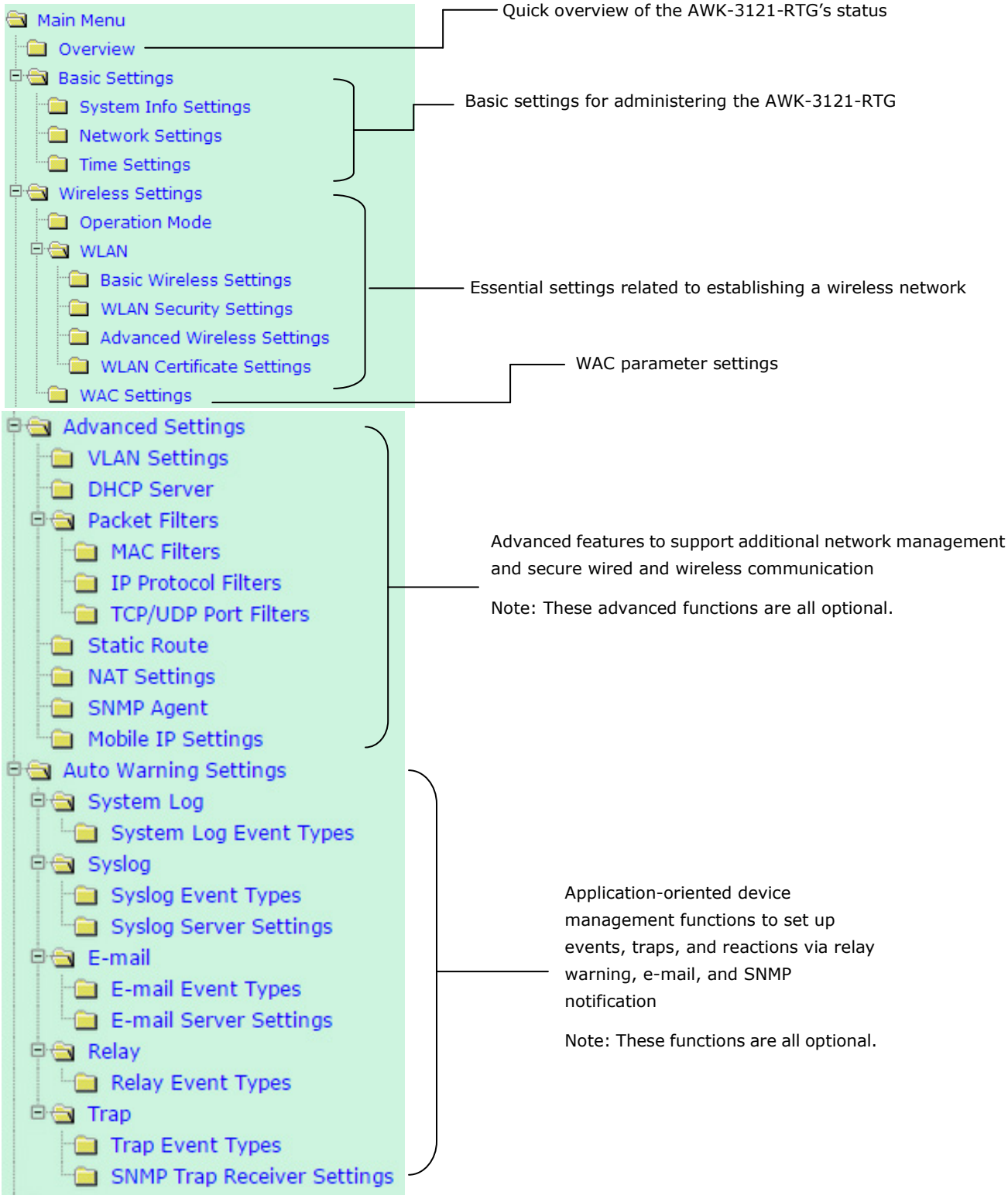


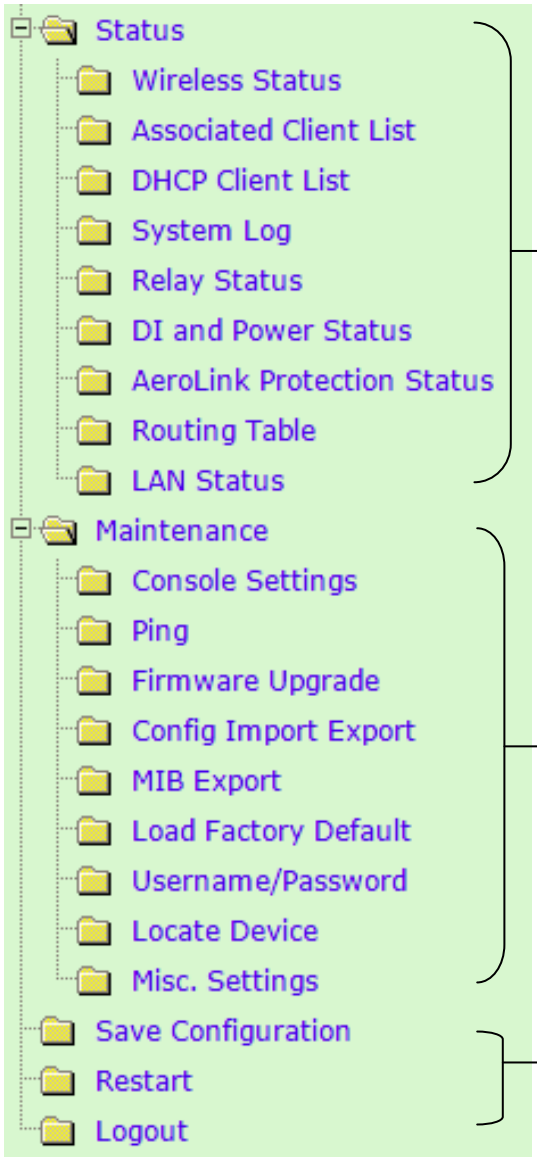
After setting up the testing environment, open a DOS window on notebook B. At the prompt, type:

ping *<IP address of notebook A>*

and then press **Enter**. A "Reply from IP address …" response means the communication was successful. A "Request timed out" response means the communication failed. In this case, recheck the configuration to make sure the connections are correct.

Function Map





Real-time status information for monitoring wired/wireless network performance, advanced services, and device management functions

Functions for maintaining the AWK-3121-RTG, and for diagnosing the network

On-demand functions to support the web-based console management operation

3

Web Console Configuration

In this chapter, we explain all aspects of web-based console configuration. Moxa's easy-to-use management functions help you set up your AWK-3121-RTG and make it easy to establish and maintain your wireless network.

The following topics are covered in this chapter:

- **Web Browser Configuration**
- **Overview**
- **Basic Settings**
  - System Info Settings
  - Network Settings
  - Time Settings
- **Wireless Settings**
  - Operation Mode
  - WLAN
  - WAC Settings
- **Advanced Settings**
  - VLAN Settings
  - Configuring Virtual LAN
  - DHCP Server (For AP mode only)
  - Packet Filters
  - Static Route (For Client-Router mode only)
  - NAT Settings/Port Forwarding (For Client-Router mode only)
  - SNMP Agent
  - Mobile IP Settings
- **Auto Warning Settings**
  - System Log
  - Syslog
  - E-mail
  - Relay
  - Trap
- **Status**
  - Wireless Status
  - Associated Client List (for AP mode only)
  - DHCP Client List (for AP mode only)
  - System Log
  - Relay Status
  - DI and Power Status
  - AeroLink Protection Status (For Client/Slave mode only)
  - Routing Table
  - LAN Status
- **Maintenance**
  - Console Settings
  - Ping
  - Firmware Upgrade
  - Config Import Export
  - Mib Export
  - Load Factory Default
  - Password
  - Locate Device
  - Misc. Settings
- **Save Configuration**
- **Restart**
- **Logout**

Web Browser Configuration

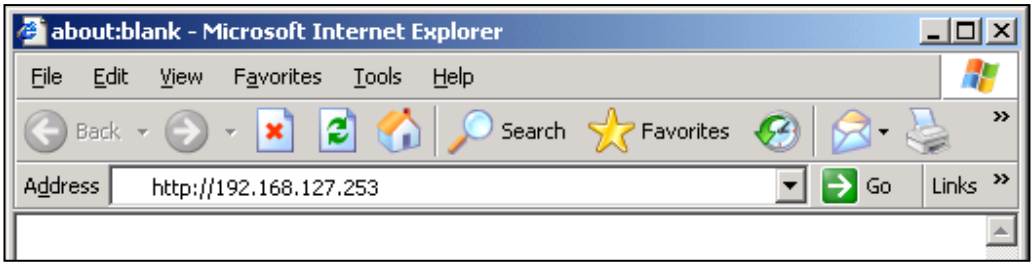
Moxa AWK-3121-RTG's web browser interface provides a convenient way to modify its configuration and access the built-in monitoring and network administration functions. The recommended web browser is Microsoft® Internet Explorer 7.0 or 8.0 with JVM (Java Virtual Machine) installed.

NOTE To use the AWK-3121-RTG's management and monitoring functions from a PC host connected to the same LAN as the AWK-3121-RTG, you must make sure that the PC host and the AWK-3121-RTG are on the same logical subnet. Similarly, if the AWK-3121-RTG is configured for other VLAN settings, you must make sure your PC host is on the management VLAN.

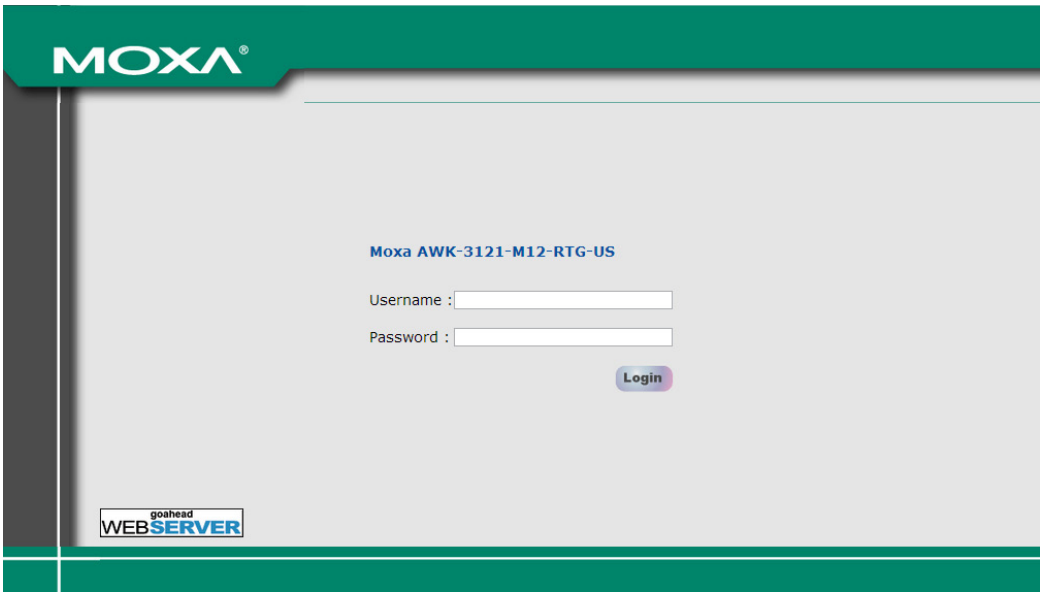
The Moxa AWK-3121-RTG's default IP is **192.168.127.253**.

Follow these steps to access the AWK-3121-RTG's web-based console management interface.

Open your web browser (e.g., Internet Explorer) and type the AWK-3121-RTG's IP address in the address field. Press **Enter** to establish the connection.

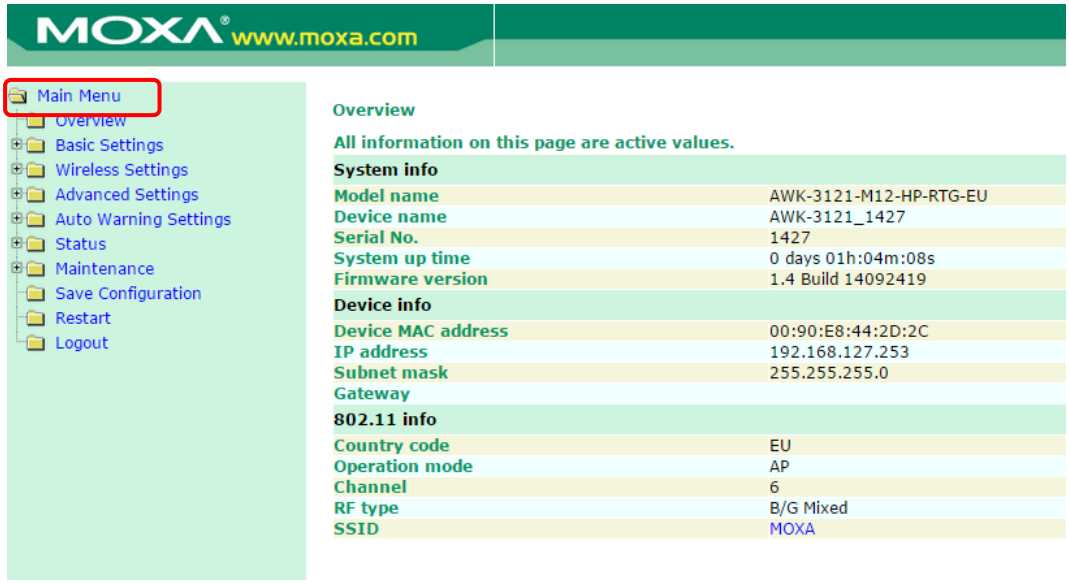


- The Web Console Login page will open. Enter the password (default Username = **admin**; default Password = **root**) and then click **Login** to continue.



1. You may need to wait a few moments for the web page to download to your computer. Note that the Model name and IP address of your AWK-3121-RTG are both shown in the title bar of the web page. This information can be used to help you identify multiple AWK-3121-RTG units.

2. Use the menu tree on the left side of the window to open the function pages to access each of the AWK-3121-RTG's functions.



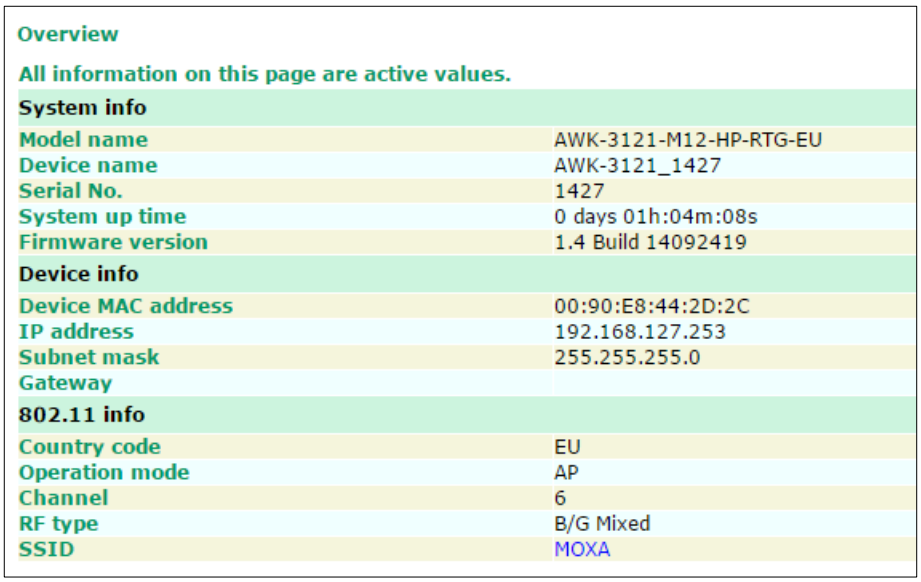
In the following paragraphs, we describe each AWK-3121-RTG management function in detail. A quick overview is available in this manual in the "Function Map" section of Chapter 2.

NOTE The model name of the AWK-3121-RTG is shown as AWK-3121-RTG-XX, where XX indicates the country code. The country code indicates the AWK-3121-RTG version and which bandwidth it uses. We use **AWK-3121-RTG-EU** as an example in the following figures. (The country code and model name that appears on your computer screen may be different than the one shown here.)

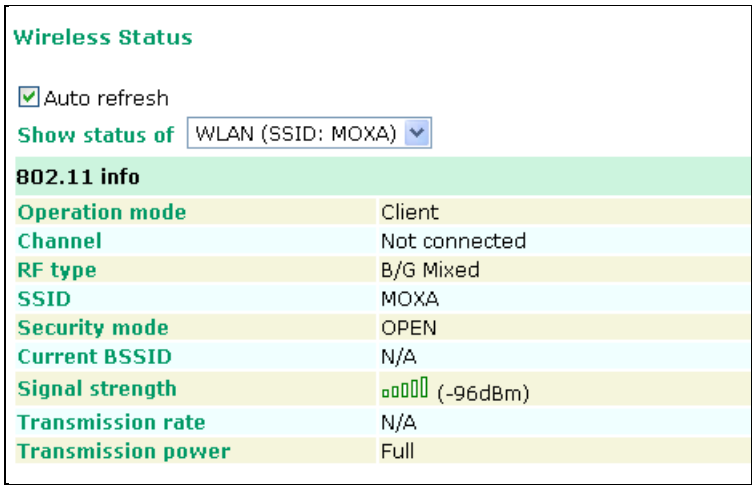
NOTE For security reasons, you will need to log back into the AWK-3121-RTG after a 5-minute time-out.

Overview

The **Overview** page summarizes the AWK-3121-RTG's current status. The information is categorized into several groups: **System info**, **Device info**, and **802.11 info**.



Click on **SSID** for more detailed 802.11 information, as shown in the following figure.



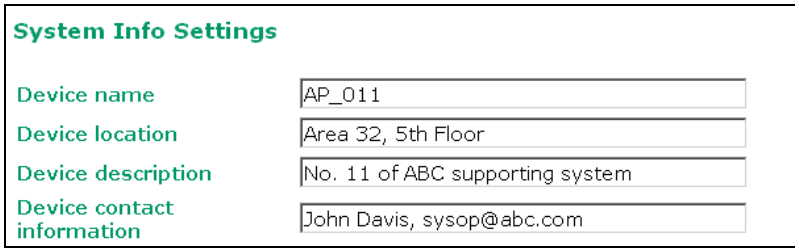
NOTE The **802.11 info** that is displayed may be different for different operation modes. For example, "Current BSSID" is not available in Client/Client Router mode, and "Signal strength" is not available in AP mode.

Basic Settings

The Basic Settings group includes the most commonly used settings required by administrators to maintain and control the AWK-3121-RTG.

System Info Settings

The **System Info** items, especially ***Device name*** and ***Device description***, are displayed and included on the **Overview** page, in SNMP information, and in alarm emails. Setting **System Info** items makes it easier to identify the different AWK-3121-RTG units connected to your network.



Device name

Setting	Description	Factory Default
Max. 31 of characters	This option is useful for specifying the role or application of different AWK-3121-RTG units.	AWK-3121-RTG_<Serial No. of this AWK-3121-RTG>

Device location

Setting	Description	Factory Default
Max. of 31 characters	Specifies the location of different AWK-3121-RTG units.	None

Device description

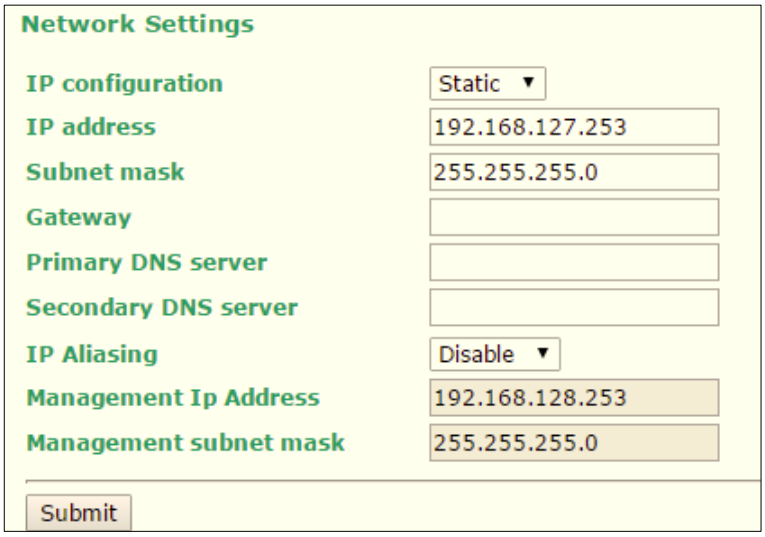
Setting	Description	Factory Default
Max. of 31 characters	Use this space to record a more detailed description of the AWK-3121-RTG	None

Device contact information

Setting	Description	Factory Default
Max. of 31 characters	Provides information about whom to contact in order to resolve problems. Use this space to record contact information of the person responsible for maintaining this AWK-3121-RTG.	None

Network Settings

The Network Settings configuration panel allows you to modify the usual TCP/IP network parameters. An explanation of each configuration item is given below.



IP configuration

Setting	Description	Factory Default
DHCP	The AWK-3121-RTG's IP address will be assigned automatically by the network's DHCP server	Static
Static	Set up the AWK-3121-RTG's IP address manually.	

IP address

Setting	Description	Factory Default
AWK-3121-RTG's IP address	Identifies the AWK-3121-RTG on a TCP/IP network.	192.168.127.253

Subnet mask

Setting	Description	Factory Default
AWK-3121-RTG's subnet mask	Identifies the type of network to which the AWK-3121-RTG is connected (e.g., 255.255.0.0 for a Class B network, or 255.255.255.0 for a Class C network).	255.255.255.0

Gateway

Setting	Description	Factory Default
AWK-3121-RTG's default gateway	The IP address of the router that connects the LAN to an outside network.	None

Primary/ Secondary DNS server

Setting	Description	Factory Default
IP address of the Primary/Secondary DNS server	The IP address of the DNS Server used by your network. After entering the DNS Server's IP address, you can input the AWK-3121-RTG's URL (e.g., http://ap11.abc.com) in your browser's address field instead of entering the IP address. The Secondary DNS server will be used if the Primary DNS server fails to connect.	None

IP Aliasing

Setting	Description	Factory Default
Enable/Disable	For device management security; use IP Aliasing to enable a separate IP address for management access only.	Disable

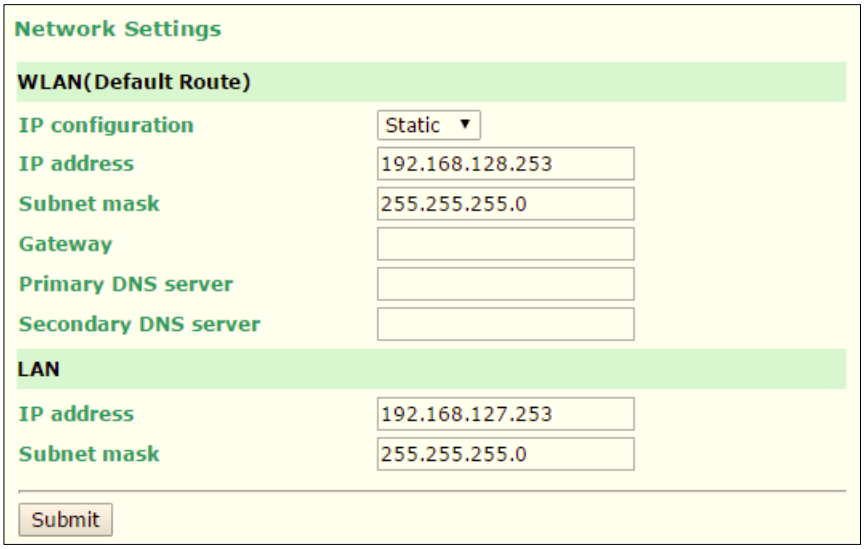
Management IP Address

Setting	Description	Factory Default
IP Address	When enabled, a management device will be able to access the AWK via this IP address.	192.168.128.253

Management Subnet Mask

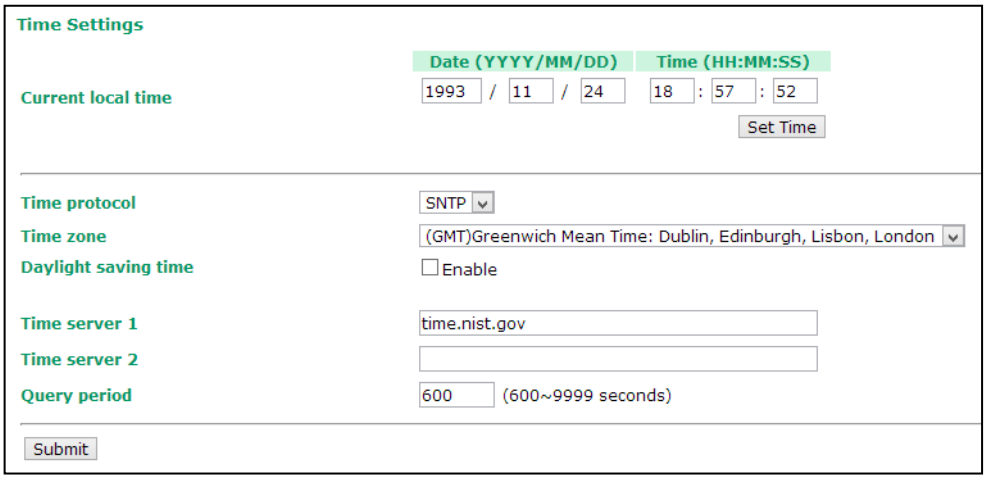
Setting	Description	Factory Default
Subnet Mask	This is the management IP's subnet mask; when enabled, a management device will be able to access the AWK via this subnet mask	255.255.255.0

NOTE When you select **Client-Router** mode, the WLAN and LAN are separated into two independent subnet interfaces. Default IP of the WLAN is 192.168.128.253 and the default IP of the LAN is 192.168.127.253.



Time Settings

The AWK-3121-RTG has a time calibration function based on information from an NTP server, SNTP server or user specified Date and Time information. Functions such as Auto warning can add real-time information to the message.



The ***Current local time*** shows the AWK-3121-RTG's system time when you open this web page. You can click on the **Set Time** button to activate the updated date and time parameters. An "(Updated)" string will appear to indicate that the change is complete. Local time settings will be immediately activated in the system without running Save and Restart.

NOTE The AWK-3121-RTG has a built-in real time clock (RTC). We strongly recommend that users update the **Local time** for the AWK-3121-RTG after the initial setup or a long-term shutdown, especially when the network does not have an Internet connection for accessing the NTP server or there is no NTP server on the LAN.

Current local time

Setting	Description	Factory Default
User adjustable time	The date and time parameters allow configuration of the local time, with immediate activation. *Use 24-hour format: yyyy/mm/dd hh:mm:ss*	None

Time zone

Setting	Description	Factory Default
User selectable time zone	The time zone setting allows conversion from GMT (Greenwich Mean Time) to local time.	GMT (Greenwich Mean Time)

ATTENTION

Changing the time zone will automatically adjust the **Current local time**. You should configure the **Time zone** before setting the **Current local time**.

Daylight saving time

Setting	Description	Factory Default
Enable/Disable	Daylight saving time (also known as DST or summer time) involves advancing clocks (usually 1 hour) during the summer time to provide an extra hour of daylight in the afternoon.	Disable

When **Daylight saving time** is enabled, the following parameters will be shown:

- **Starts at:** The date that daylight saving time begins.
- **Stops at:** The date that daylight saving time ends.
- **Time offset:** Indicates how many hours forward the clock should be advanced.

Time server 1/2

Setting	Description	Factory Default
IP/Name of Time Server 1/2	IP or Domain name of the NTP or SNTP time server. The 2nd NTP OR SNTP time server will be used if the 1st NTP or SNTP server fails to connect.	None

Query period

Setting	Description	Factory Default
Query period time (1 to 9999 seconds)	This parameter determines how often the time is updated from the NTP or SNTP server.	600 (seconds)

Wireless Settings

The essential settings for wireless networks are presented in this function group. Settings must be properly set before establishing your wireless network. Familiarize yourself with the following terms before starting the configuration process:

AP: This mode provides both Access Point and Static LAN-to-LAN Bridging functionality.

Client/Client-Router: These modes are for Dynamic LAN-to-LAN Bridging or Device-to-LAN scenarios. The Client automatically establishes bridge links with other APs.

In AP, Client, or Client-Router mode, the AWK-3121-RTG forwards packets between its Ethernet interface (LAN) and wireless interface (WLAN) to connect wired hosts on the Ethernet side with wireless host(s) on the wireless side. Two types of wireless links are specified by the IEEE 802.11 standard:

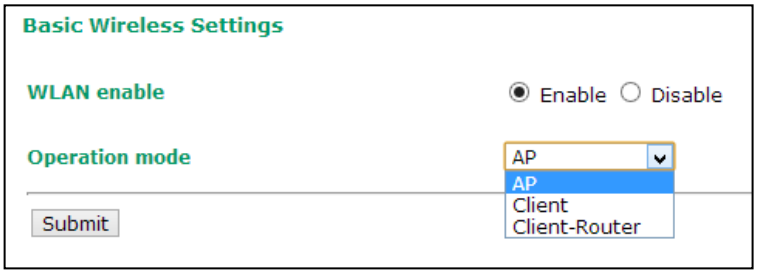
STA AP: This type of wireless link is established between an IEEE 802.11 Station (STA) and an IEEE 802.11 Access Point (AP). An STA is usually a client computer (PC or PDA) with a WLAN network interface card (NIC). The Client mode is actually an STA.

When the AWK-3121-RTG is configured for **Client or Client-Router** mode, it can be used as an Ethernet-to-wireless (or LAN-to-WLAN) network adapter. For example, a notebook computer equipped with an Ethernet adapter but no wireless card can be connected to this device with an Ethernet cable to provide wireless connectivity to another AP.

NOTE Although it is more convenient to use dynamic bridging, there is a limitation—the AP Client can only transmit IP-based packets between its wireless interface (WLAN) and Ethernet interface (LAN); other types of traffic (such as IPX and AppleTalk) are not forwarded.

Operation Mode

The AWK-3121-RTG supports three main operation modes—AP, Client, and Client-Router—each mode plays a distinct role on the wireless network.



WLAN Enable

Setting	Description	Factory Default
Enable/Disable	The RF (Radio Frequency) module can be manually turned on or off. This function is available in AP operation mode only.	Enable

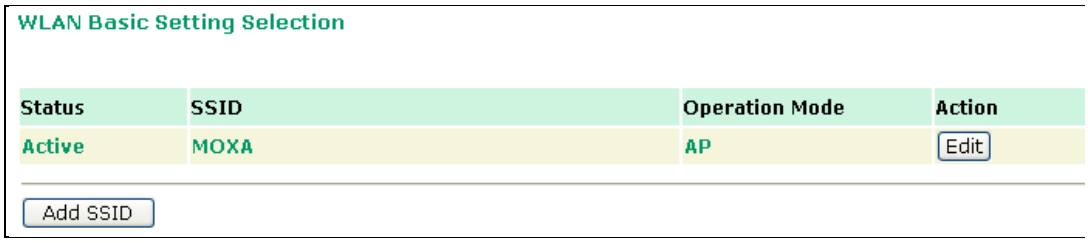
Operation Mode

Setting	Description	Factory Default
AP	The AWK-3121-RTG plays the role of wireless AP	AP
Client	The AWK-3121-RTG plays the role of wireless Client	
Client-Router	The AWK-3121-RTG plays the role of wireless Client and Router.	

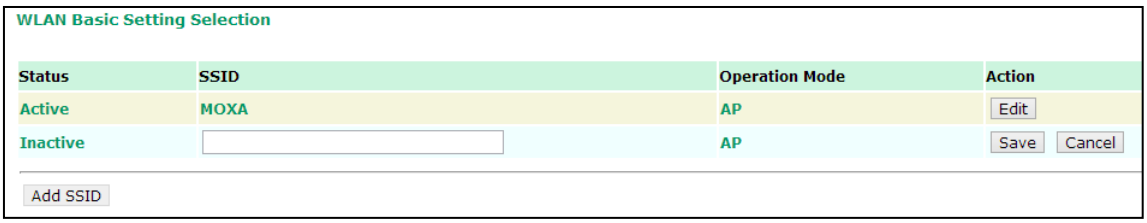
WLAN

Basic Wireless Settings

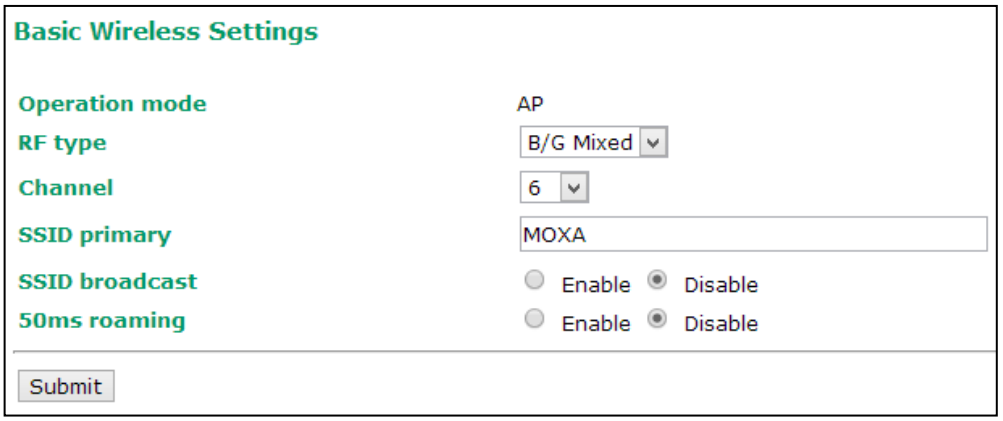
The "WLAN Basic Setting Selection" panel is used to add and edit SSIDs. An SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Multiple access points on a network or sub-network can use the same SSIDs. You can configure your AWK to use up to 9 SSIDs, and configure each SSID differently. All of the SSIDs are active at the same time; that is, client devices can use any of the SSIDs to associate with the access point.



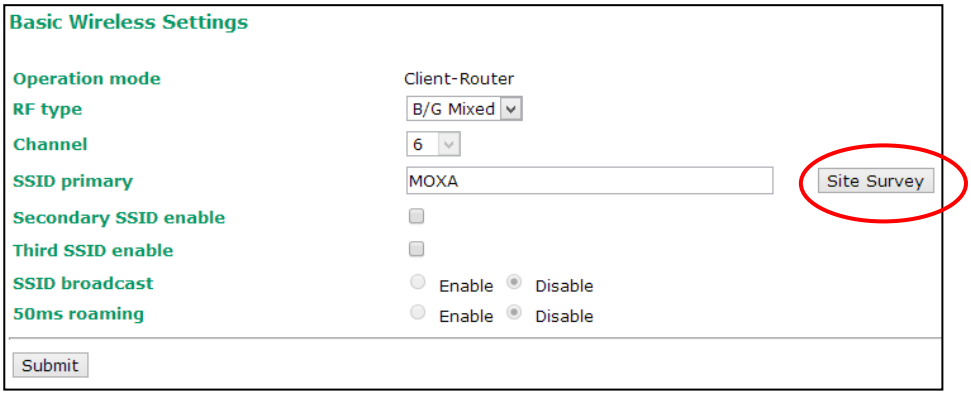
Click on **Add SSID** to create more SSIDs.

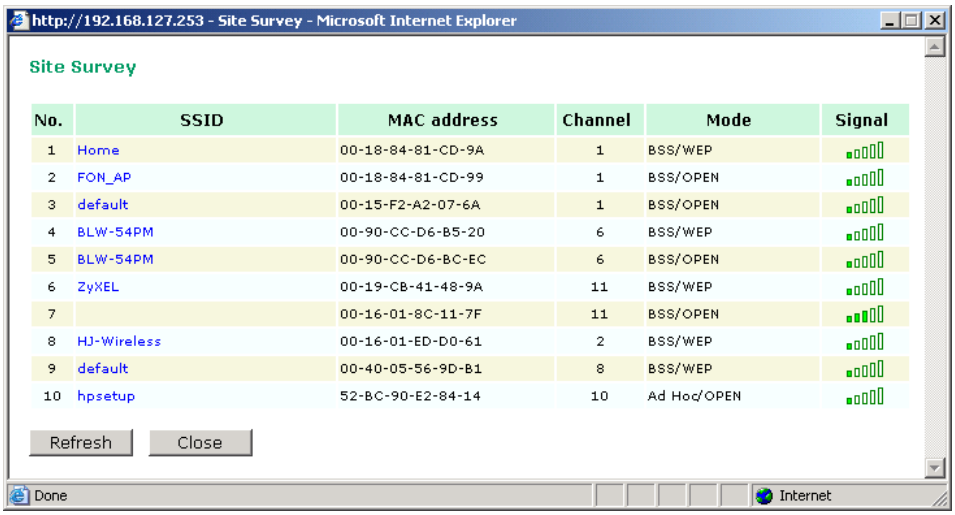


Click on **Edit** to assign different configuration settings to each SSID. The configuration panel appears as follows:



NOTE When you switch to **Client** or **Client-Router** mode, a **Site Survey** button will be available on the Basic Wireless Settings panel. Click the "Site Survey" button to view information about available APs, as shown in the following figure. You can click on the SSID of an entity and bring the value of its SSID onto the SSID field of the Basic Wireless Settings page. Click the **Refresh** button to re-scan and update the table. If this client is connecting to an AP, a brief disconnection will occur during a site survey.





NOTE If the **Gateway** field in **Basic Settings → Network Settings** is empty, a warning message will appear, reminding you to set the default gateway when **Client** mode is enabled. You can ignore this message if you are only planning a local network and packets will not be sent outside the network.

RF type

Setting	Description	Factory Default
A	Supports the IEEE 802.11a standard only	B/G Mixed
B	Supports the IEEE 802.11b standard only	
G	Supports the IEEE 802.11g standard only	
B/G Mixed	Supports both IEEE 802.11b/g standards, but 802.11g can be slowed down when 802.11b clients are on the network	

Channel (for AP mode only)

Setting	Description	Factory Default
Available channels vary with RF type	AWK-3121-RTG plays a role of wireless AP.	6 (in B/G Mixed mode)

SSID

Setting	Description	Factory Default
Max. of 31 characters	The SSID of a client and the SSID of the AP must be identical for the client and AP to be able to communicate with each other.	MOXA

SSID broadcast (For AP mode only)

Setting	Description	Factory Default
Enable/ Disable	Determines whether or not the SSID can be broadcast	Enable

NOTE The AWK-3121-RTG-EU (for European frequency bands) only connects SSID-hidden APs on all IEEE 802.11b/g channels.

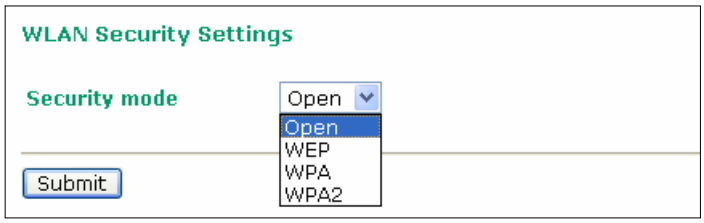
50 ms roaming (only works with the WAC-1001, WAC-2004, and RTG series)

Setting	Description	Factory Default
Enable/Disable	Determines whether or not the AWK-3121-RTG supports 50 ms roaming.	Disable

WLAN Security Settings

The AWK-3121-RTG provides four standardized wireless security modes: **Open**, **WEP** (Wired Equivalent Privacy), **WPA** (Wi-Fi Protected Access), and **WPA2**. Several security modes are available in the AWK-3121-RTG by selecting ***Security mode*** and ***WPA type***:

- **Open:** No authentication, no data encryption.
- **WEP:** Static WEP (Wired Equivalent Privacy) keys must be configured manually.
- **WPA/WPA2-Personal:** Also known as WPA/WPA2-PSK. You will need to specify the Pre-Shared Key in the ***Passphrase*** field, which will be used by the TKIP or AES engine as a master key to generate keys that actually encrypt outgoing packets and decrypt incoming packets.
- **WPA/WPA2-Enterprise:** Also called WPA/WPA2-EAP (Extensible Authentication Protocol). In addition to device-based authentication, WPA/WPA2-Enterprise enables user-based authentication via IEEE 802.1X. The AWK-3121-RTG can support three EAP methods: EAP-TLS, EAP-TTLS, and EAP-PEAP.



NOTE 50 ms roaming only works in WPA and WPA2 modes.

Security mode

Setting	Description	Factory Default
Open	No authentication	Open
WEP	Static WEP is used	
WPA*	WPA is used	
WPA2*	Fully supports IEEE 802.11i with "TKIP/AES + 802.1X"	

Open

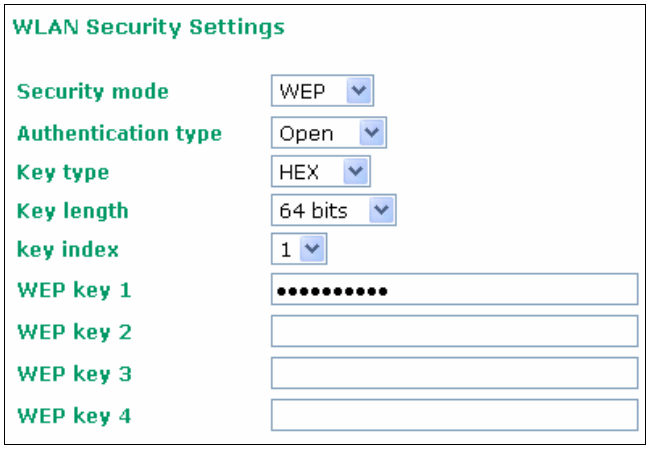
For security reasons, you should **NOT** set security mode to Open System, since authentication and data encryption are **NOT** performed in Open System mode.

WEP

According to the IEEE 802.11 standard, WEP can be used for authentication and data encryption to maintain confidentiality. **Shared** (or **Shared Key**) authentication type is used if WEP authentication and data encryption are both needed. Normally, **Open** (or **Open System**) authentication type is used when WEP data encryption is run with authentication.

When WEP is enabled as a security mode, the length of a key (so-called WEP seed) can be specified as 64/128 bits, which is actually a 40/104-bit secret key with a 24-bit initialization vector. The AWK-3121-RTG provides 4 entities of WEP key settings that can be selected to use with ***Key index***. The selected key setting specifies the key to be used as a *send-key* for encrypting traffic from the AP side to the wireless client side. All 4 WEP keys are used as *receive-keys* to decrypt traffic from the wireless client side to the AP side.

The WEP key can be presented in two ***Key types***, HEX and ASCII. Each ASCII character has 8 bits, so a 40-bit (or 64-bit) WEP key contains 5 characters, and a 104-bit (or 128-bit) key has 13 characters. In hex, each character uses 4 bits, so a 40-bit key has 10 hex characters, and a 128-bit key has 26 characters.



Authentication type

Setting	Description	Factory Default
Open	Data encryption is enabled, but without authentication	Open
Shared	Data encryption and authentication are both enabled	

Key type

Setting	Description	Factory Default
HEX	Specifies WEP keys in hex-decimal number form	HEX
ASCII	Specifies WEP keys in ASCII form	

Key length

Setting	Description	Factory Default
64 bits	Uses 40-bit secret keys with 24-bit initialization vector	64 bits
128 bits	Uses 104-bit secret key with 24-bit initialization vector	

Key index

Setting	Description	Factory Default
1-4	Specifies which WEP key is used	Open

WEP key 1-4

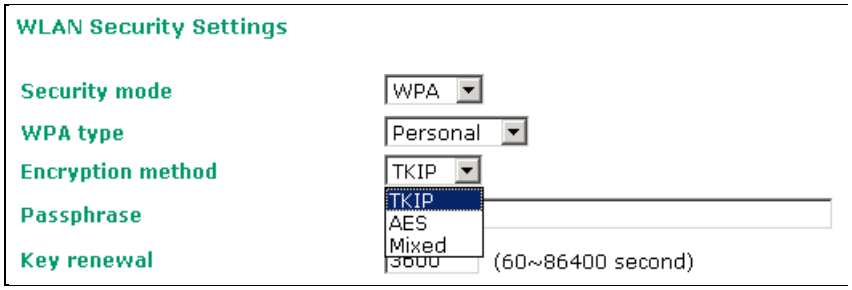
Setting	Description	Factory Default
ASCII type: 64 bits: 5 chars 128 bits: 13 chars HEX type: 64 bits: 10 hex chars 128 bits: 26 hex chars	A string that can be used as a WEP seed for the RC4 encryption engine.	None

WPA/WPA2-Personal

WPA (Wi-Fi Protected Access) and WPA2 represent significant improvements over the WEP encryption method. WPA is a security standard based on 802.11i draft 3, while WPA2 is based on the fully ratified version of 802.11i. The initial vector is transmitted, encrypted, and enhanced with its 48 bits, twice as long as WEP. The key is regularly changed so that the session is secure.

Even though AES encryption is only included in the WPA2 standard, it is widely available in the WPA security mode of some wireless APs and clients as well. The AWK-3121-RTG also supports AES algorithms in WPA and WPA2 for better compatibility.

Personal versions of WPA/WPA2, also known as WPA/WPA-PSK (*Pre-Shared Key*), provide a simple way of encrypting a wireless connection for high confidentiality. A ***Passphrase*** is used as a basis for encryption methods (or cipher types) in a WLAN connection. The passphrases should be complicated and as long as possible. There must be at least 8 ASCII characters in the Passphrase, and it can be as long as 63. For security reasons, this passphrase should only be disclosed to users who need it, and it should be changed regularly.



WPA type

Setting	Description	Factory Default
Personal	Provides Pre-Shared Key-enabled WPA and WPA2	Personal
Enterprise	Provides enterprise-level security for WPA and WPA2	

Encryption method

Setting	Description	Factory Default
TKIP	Temporal Key Integrity Protocol is enabled	TKIP
AES	Advanced Encryption System is enabled	
Mixed*	Provides a TKIP broadcast key and TKIP+AES unicast key for some legacy AP clients. This option is rarely used.	

**This option is only available in AP mode, and does not support AES-enabled clients.*

Passphrase

Setting	Description	Factory Default
8 to 63 characters	Master key to generate keys for encryption and decryption	None

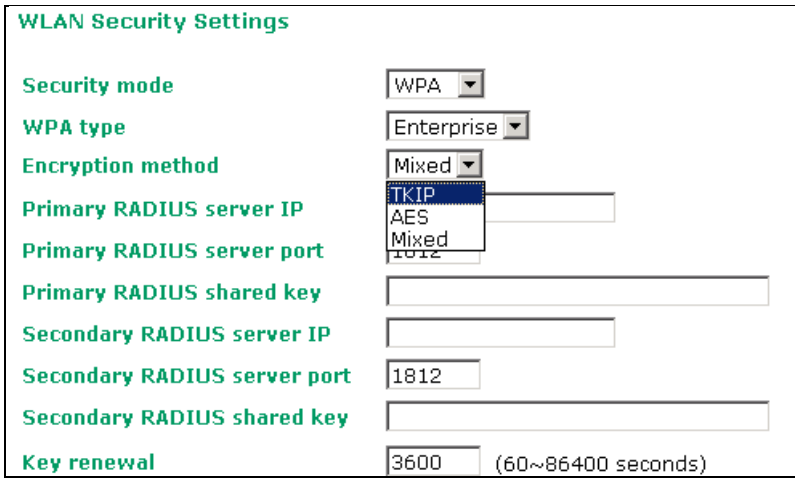
Key renewal (For AP mode only)

Setting	Description	Factory Default
60 to 86400 seconds (1 minute to 1 day)	Specifies the time period of group key renewal	3600 (seconds)

NOTE The ***key renewal*** value dictates how often the wireless AP encryption keys should be changed. The security level is generally higher if you set the key renewal value to a shorter number, which forces the encryption keys to be changed more frequently. The default value is 3600 seconds (6 minutes). Longer time periods can be considered if the line is not very busy.

WPA/WPA2-Enterprise (For AP mode only)

By setting ***WPA type*** to **Enterprise**, you can use **EAP** (*Extensible Authentication Protocol*), a framework authentication protocol used by 802.1X to provide network authentication. In these Enterprise-level security modes, a back-end RADIUS (Remote Authentication Dial-In User Service) server is needed if IEEE 802.1X functionality is enabled in WPA /WPA2. The IEEE 802.1X protocol also offers the possibility of carrying out an efficient connection authentication on a large-scale network. It is not necessary to exchange keys or passphrases.



WPA type

Setting	Description	Factory Default
Personal	Provides Pre-Shared Key-enabled WPA and WPA2	Personal
Enterprise	Provides enterprise-level security for WPA and WPA2	

Encryption method

Setting	Description	Factory Default
TKIP	Temporal Key Integrity Protocol is enabled	TKIP
AES	Advance Encryption System is enabled	
Mixed*	Provides TKIP broadcast key and TKIP+AES unicast key for some legacy AP clients. This option is rarely used.	

**This option is available in AP mode only, and cannot support AES-enabled clients.*

Primary/Secondary RADIUS server IP

Setting	Description	Factory Default
The IP address of RADIUS server	Specifies the delegated RADIUS server for EAP	None

Primary/Secondary RADIUS port

Setting	Description	Factory Default
Port number	Specifies the port number of the delegated RADIUS server	1812

Primary/ Secondary RADIUS shared key

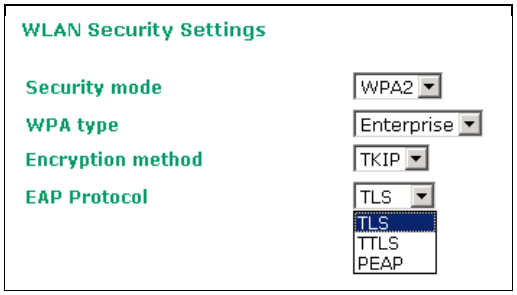
Setting	Description	Factory Default
Max. of 31 characters	The secret key shared between AP and RADIUS server	None

Key renewal

Setting	Description	Factory Default
60 to 86400 seconds (1 minute to 1 year)	Specifies the time period of group key renewal	3600 (seconds)

WPA/WPA2-Enterprise (for Client/Slave mode)

When used as a client, the AWK-3121-RTG can support three EAP methods (or ***EAP protocols***): **EAP-TLS**, **EAP-TTLS**, and **EAP-PEAP**, corresponding to WPA/WPA-Enterprise settings on the AP side.



Encryption method

Setting	Description	Factory Default
TKIP	Temporal Key Integrity Protocol is enabled	TKIP
AES	Advance Encryption System is enabled	

EAP Protocol

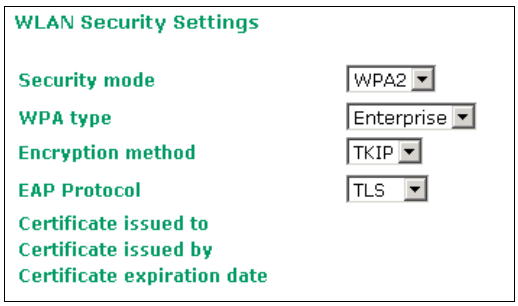
Setting	Description	Factory Default
TLS	Specifies Transport Layer Security protocol	TLS
TTLS	Specifies Tunneled Transport Layer Security	
PEAP	Specifies Protected Extensible Authentication Protocol, or Protected EAP	

Before choosing the EAP protocol for your WPA/WPA2-Enterprise settings on the client end, please contact the network administrator to make sure the system supports the protocol on the AP end. Detailed information on these three popular EAP protocols is presented in the following sections.

EAP-TLS

TLS is the standards-based successor to Secure Socket Layer (SSL). It can establish a trusted communication channel over a distrusted network. TLS provides mutual authentication through certificate exchange. EAP-TLS is also secure to use. You are required to submit a digital certificate to the authentication server for validation, but the authentication server must also supply a certificate.

You can use **Basic Wireless Settings** → **WLAN Certificate Settings** to import your WLAN certificate and enable EAP-TLS on the client end.



You can check the current certificate status in ***Current Status*** if it is available.

- **Certificate issued to:** Shows the certificate user
- **Certificate issued by**: Shows the certificate issuer
- **Certificate expiration date**: Indicates when the certificate has expired

EAP-TTLS

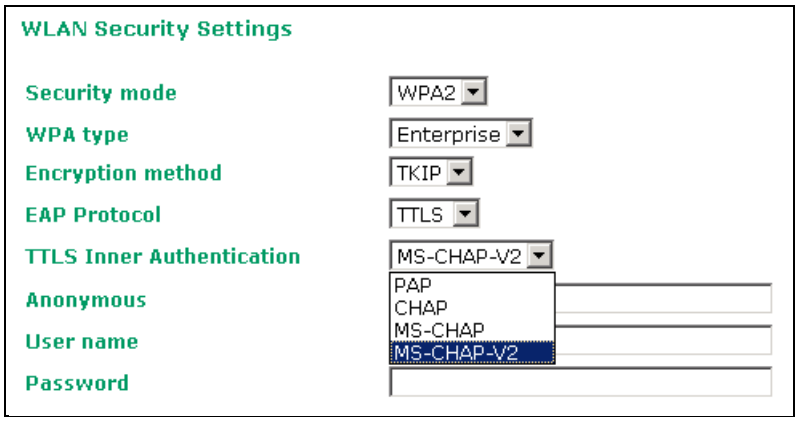
It is usually much easier to re-use existing authentication systems, such as a Windows domain or Active Directory, LDAP directory, or Kerberos realm, rather than creating a parallel authentication system. As a result, TTLS (Tunneled TLS) and PEAP (Protected EAP) are used to support the use of so-called "legacy authentication methods."

TTLS and PEAP work in a similar way. First, they establish a TLS tunnel (EAP-TLS for example), and validate whether the network is trustworthy with digital certificates on the authentication server. This step establishes a tunnel that protects the next step (or "inner" authentication), and consequently is sometimes referred to as "outer" authentication. The TLS tunnel is then used to encrypt an older authentication protocol that authenticates the user for the network.

As you can see, digital certificates are still needed for outer authentication in a simplified form. Only a small number of certificates are required, which can be generated by a small certificate authority. Certificate reduction makes TTLS and PEAP much more popular than EAP-TLS.

The AWK-3121-RTG provides some non-cryptographic EAP methods, including **PAP**, **CHAP**, **MS-CHAP**, and **MS-CHAP-V2**. These EAP methods are not recommended for direct use on wireless networks. However, they may be useful as inner authentication methods with TTLS and PEAP.

Because the inner and outer authentications can use distinct user names in TTLS and PEAP, you can use an anonymous user name for the outer authentication, with the true user name only shown through the encrypted channel. Keep in mind that not all client software supports anonymous alteration. Confirm this with the network administrator before you enable identity hiding in TTLS and PEAP.



TTL Inner Authentication

Setting	Description	Factory Default
PAP	Password Authentication Protocol is used	MS-CHAP-V2
CHAP	Challenge Handshake Authentication Protocol is used	
MS-CHAP	Microsoft CHAP is used	
MS-CHAP-V2	Microsoft CHAP version 2 is used	

Anonymous

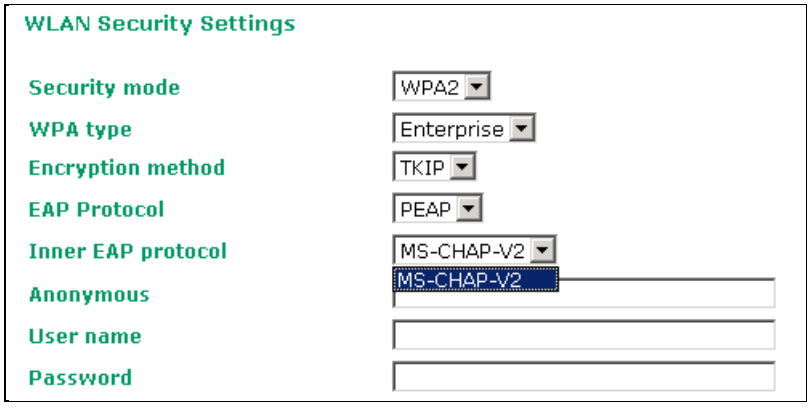
Setting	Description	Factory Default
Max. of 31 characters	A distinct name used for outer authentication	None

User name & Password

Setting	Description	Factory Default
	User name and password used in inner authentication	None

PEAP

There are a few differences in the TTLS and PEAP inner authentication procedures. TTLS uses the encrypted channel to exchange attribute-value pairs (AVPs), while PEAP uses the encrypted channel to start a second EAP exchange inside of the tunnel. The AWK-3121-RTG provides **MS-CHAP-V2** merely as an EAP method for inner authentication.



Inner EAP protocol

Setting	Description	Factory Default
MS-CHAP-V2	Microsoft CHAP version 2 is used	MS-CHAP-V2

Anonymous

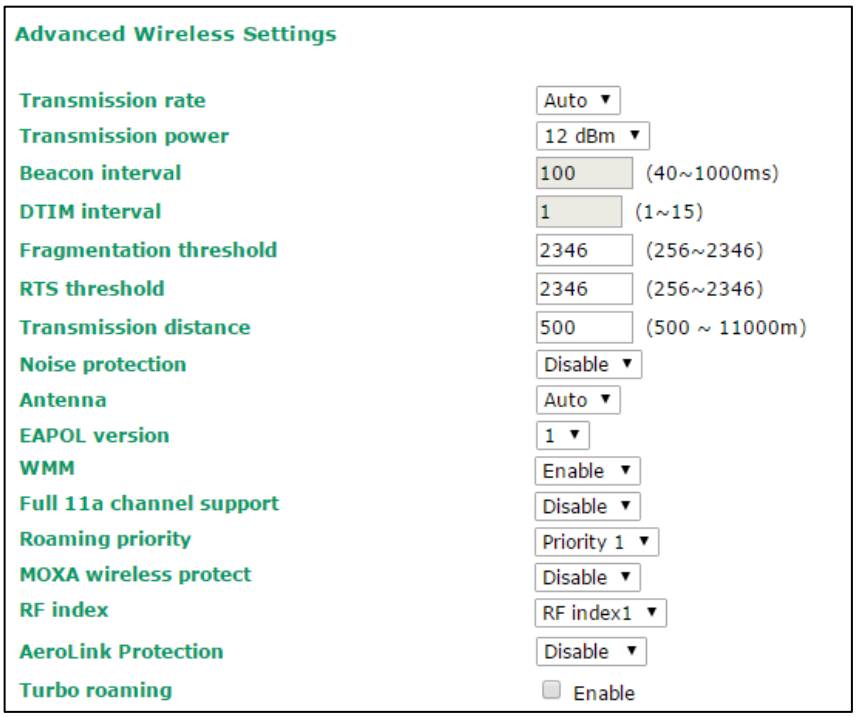
Setting	Description	Factory Default
Max. of 31 characters	A distinct name used for outer authentication	None

User name & Password

Setting	Description	Factory Default
	User name and password used in inner authentication	None

Advanced Wireless Settings

Additional wireless-related parameters are presented in this section to help you set up your wireless network in detail.



Transmission Rate

Setting	Description	Factory Default
Auto	The AWK-3121-RTG senses and adjusts the data rate automatically	Auto
Available rates	Users can manually select a target transmission data rate	

Transmission Power

Setting	Description	Factory Default
Available power	Users can manually select a target power to mask max output power. Because different transmission rate would have it own max output power, please reference product datasheet. For 802.11bg, the available setting is from 0 to 22 For 802.11a, the available setting is from 0 to 17	12

Beacon Interval (for AP mode only)

Setting	Description	Factory Default
Beacon Interval (40 to 1000 ms)	Indicates the frequency interval of the beacon	100 (ms)

DTIM Interval (for AP mode only)

Setting	Description	Factory Default
Data Beacon Rate (1 to 15)	Indicates how often the AWK-3121-RTG sends out a Delivery Traffic Indication Message	1

Fragmentation threshold

Setting	Description	Factory Default
Fragment Length (256 to 2346)	Specifies the maximum size a data packet before splitting and creating another new packet	2346

RTS threshold

Setting	Description	Factory Default
RTS/CTS Threshold (256 to 2346)	Determines how large a packet can be before the Access Point coordinates transmission and reception to ensure efficient communication	2346

NOTE **Transmission power** indicates the maximum value of transmission power which the user plans. However, the real transmitted power depends on the radio module and some facts, such as country, regulatory limitations and data rate. Please check the ***Transmission power*** in **Status → Wireless Status** for a real and updated value of transmission power, which the AWK is currently using.

You can refer to the related glossaries in the reference section for detailed information about the above-mentioned settings. By setting these parameters properly, you can better tune the performance of your wireless network.

Transmission distance

Setting	Description	Factory Default
Distance or max. range for transmission (500 to 11000 m)	Specifies the transmission distance or max. range between two AWK devices. This parameter should be set properly, especially for long-distance communication.	500

Noise protection

Setting	Description	Factory Default
Enable/Disable	Adjusts the interference coping capability of the wireless signal. This option should be enabled for communication distance under 500 meters, and should be disabled for communication distances over 500 meters.	Disable

NOTE Make sure the same **Transmission distance** parameters are set in both **AP** and **Client** sides. When this parameter is greater than 500, an optimal algorithm will be enabled to support long-distance transmission.

Note that **Transmission enhancement** only supports **802.11b/g** mode; **802.11a** mode is not supported.

Transmission enhancement is also recommended to enable communication at both ends when long-distance transmission is required. A high-gain antenna installed at a fixed antenna connector can also improve performance. (Select **Antenna** at MAIN or AUX.)

Antenna

Setting	Description	Factory Default
Auto	The AWK-3121-RTG uses two antennas (MAIN and AUX) and enables the diversity function for reducing multipath effect.	Auto
MAIN	Diversity function is disabled. Only MAIN antenna is in use.	
AUX	Diversity function is disabled. Only AUX antenna is in use.	

EAPOL Version

Setting	Description	Factory Default
1	EAPOL version 1 was standardized in the 2001 version of 802.1X, which is much more commonly implemented.	1
2	EAPOL version 2 was specified in 802.1X-2004.	

WMM

Setting	Description	Factory Default
Enable/Disable	WMM is a QoS standard for WLAN traffic. Voice and video data will be given priority bandwidth when enabled with WMM supported wireless clients.	Disable

Full 11a channel support

Setting	Description	Factory Default
Enable/Disable	"Full 11a channel support" allows users to select one channel from 802.11a, including channels in licensed and unlicensed bands.	Disable

READ THIS BEFORE CHANGING THE DFS SETTING

DFS (Dynamic Frequency Selection) is a mechanism to allow unlicensed wireless devices to share spectrum with existing radar systems by detecting radar systems and avoid causing interference with them. The current versions of Moxa AWK series products do not support DFS, so only U-NII Low channels (36, 40, 44, and 48) are supported by default. If you want to enable the "Full 11a channel support" option, keep in mind that your wireless devices may interfere with radar systems, which may violate local laws. If you are not sure about this, we recommend that you keep this option disabled. Updated firmware that supports DFS will be available soon.

Roaming Priority (Only for AP mode)

Setting	Description	Factory Default
Priority 1/2	The roaming priority should be set based on how the radios are deployed along the trackside. Priority 1: radios along the trackside are deployed with open air radiating antennas. Prioirity 2: radios along the trackside are deployed with leaky feeder like coverage patterns. Due to the differences in coverage patterns between different deployment scenarios, the roaming priority you select will impact roaming performance.	Priority 2

MOXA wireless protect

Setting	Description	Factory Default
Enable/ Disable	Enables Moxa's Wireless Protect feature to protect your wireless network from DoS attacks. This function only works with Moxa's AWK-RTG series.	Disable

RF Index

Setting	Description	Factory Default
RF Index1/ RF Index 2	In an L3 roaming scenario, trackside APs can be arranged in different VLAN gateways within different subnets. The RF index setting identifies the AP within a particular VLAN gateway.	RF Index 1

AeroLink Protection

Setting	Description	Factory Default
Disable/L2/L3	• Enable AeroLink Protection to allow wireless clients on the same LAN network to automatically negotiate with each other and form a redundant wireless communication. For more details, see Status → AeroLink Protection Status. • Select L2 for roaming on an L2 trackside network. • Select L3 for roaming on an L3 trackside network.	Disabled

When L3 is selected, Virtual LAN IP and Virtual WLAN IP are shown as additional setting parameters.

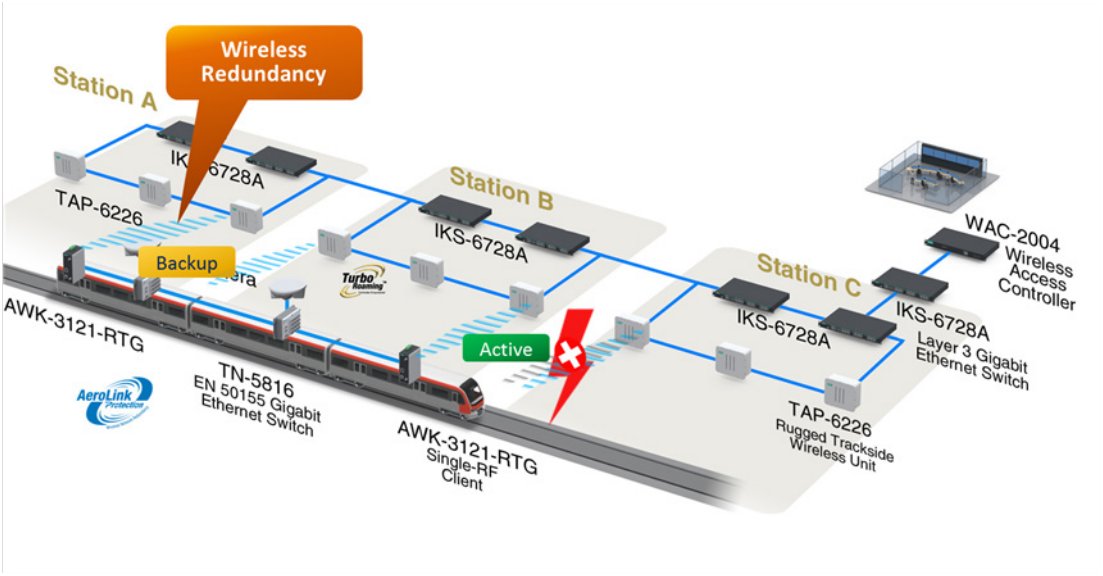
Virtual LAN IP: This IP should be defined as the gateway IP for onboard devices so that all incoming and outgoing traffic can be routed properly via this common IP in case of any role changes of the onboard clients. All AeroLink protected clients within the same subnet need to be configured with the same virtual LAN IP.

Virtual WLAN IP: This IP should be defined as the virtual gateway IP for the wayside router, which can route traffic to any onboard client regardless of the client's home WAC. This IP only needs to be configured when case different clients are to backup each other while the clients are registered to different WAC units. For the router work properly, all clients and the wayside router will need to be configured to have this routing rule (i.e., to use this virtual WLAN IP).

How AeroLink Protection works.

In vehicle-to-ground applications, it is essential to minimize system downtime and maximize system availability of the train to ground link to ensure proper communication. Moxa's AeroLink Protection provides a reliable wireless network-level redundancy protocol to ensure that there will always be a live onboard-to-ground link, even when failures occur:

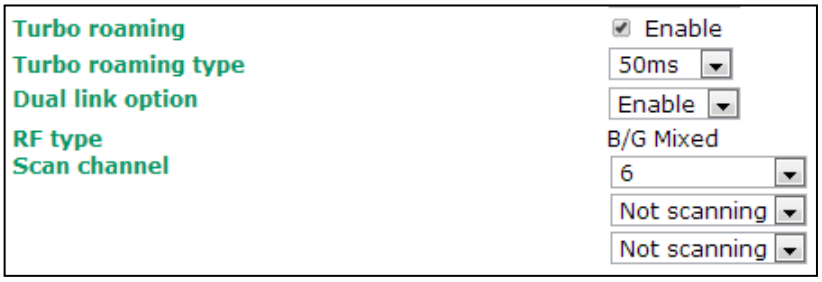
1. Communication Failover: AeroLink Protection members can negotiate with each other to automatically elect an Active node for data communication. If the Active node is no long capable of sending data across to its access point, it will inform other Backup nodes to resume the communication via another path.
2. Frequency-Interference Failover: This concept is similar to "Communication Failover." If the communication frequency is interfered with and data can no longer transmit over the Active frequency, it will also resume the connection via another Backup frequency.
3. Device Failover: After handling communication and frequency failures, in order to provide a wireless network free of single points of failure, AeroLink Protection also checks the device status. If the Active node has a power failure, the Backup nodes will automatically resume the wireless communication.
4. Scalable: AeroLink Protection is designed to allow multiple backup paths, making it possible for users to realize a complete redundant wireless network free from all the above failure types.
5. Fast Recovery: In addition to maintaining a redundant wireless network, equally important is providing uninterrupted communication even when a failure occurs. AeroLink Protection is designed to recover any failure in under 300 ms.



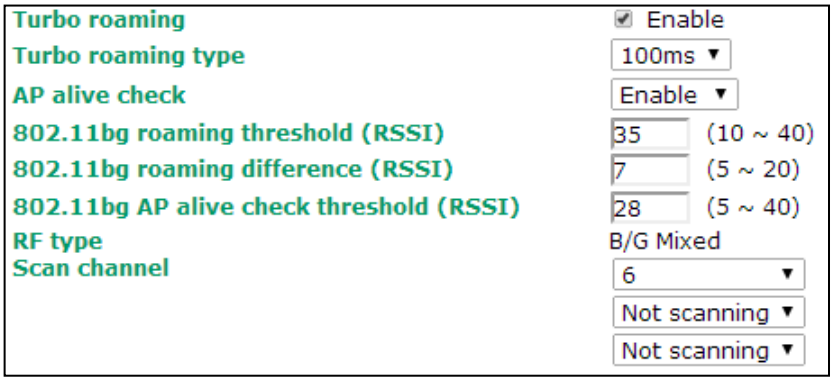
Turbo Roaming

Setting	Description	Factory Default
Enable/ Disable	Moxa's Turbo Roaming can enable rapid handover when the AWK-3121-RTG, as a client or client-router, roams among a group of APs.	Disable

When Turbo Roaming is enabled, **Turbo roaming type**, the **RF type**, **Dual link option**, and **Scan channels** will be shown as follows. There are two **Turbo roaming types** available. 50 ms Turbo roaming only works with the RTG version of the access point and the WAC-1001 and WAC-2004. 100 ms Turbo roaming supports all brands of AP. **Dual link** reduces the packet-loss rate when roaming between difference APs; this function only works with a single channel roaming structure. The RF type shows the current **RF type** that this client is using. There are three Scan channels available. Note that the **Scan channels** may need to be modified when the **RF type** is changed. (For example, channel 36 is not available in **B**, **G**, or **B/G Mix** mode.)



If you select to 100ms Turbo roaming, there are three roaming parameters, 802.11b/g (or a) roaming threshold, 802.11b/g (or a) roaming offset and 802.11b/g (or a) roaming alive would be shown as follows



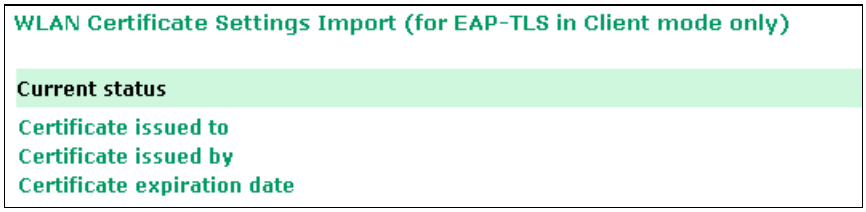
Roaming Parameters

Setting	Description	Factory Default
802.11b/g (or a) roaming threshold	When current linking RSSI is lower than this value Client would start the roaming process.	35
802.11b/g (or a) roaming offset	In roaming process when RSSI of a candidate is higher current linking RSSI more than roaming offset value then Client would roam to this new candidate.	7
802.11b/g (or a) roaming rssi alive	When roaming process is triggered, the RSSI value what Client could get from air is higher than rssi alive would be the roaming candidate.	28

NOTE When 50 ms Turbo Roaming is enabled without using the WAC-1001 or WAC-2004, the connection between the AP and client will not work.

WLAN Certification Settings (for EAP-TLS in Client mode only)

When EAP-TLS is used, a WLAN Certificate will be required at the client end to support WPA/WPA2-Enterprise. The AWK-3121-RTG can support the **PKCS #12**, also known as *Personal Information Exchange Syntax Standard*, certificate formats that define file formats commonly used to store private keys with accompanying public key certificates, protected with a password-based symmetric key.



Current Status displays information for the current WLAN certificate, which has been imported into the AWK-3121-RTG. Nothing will be shown if a certificate is not available.

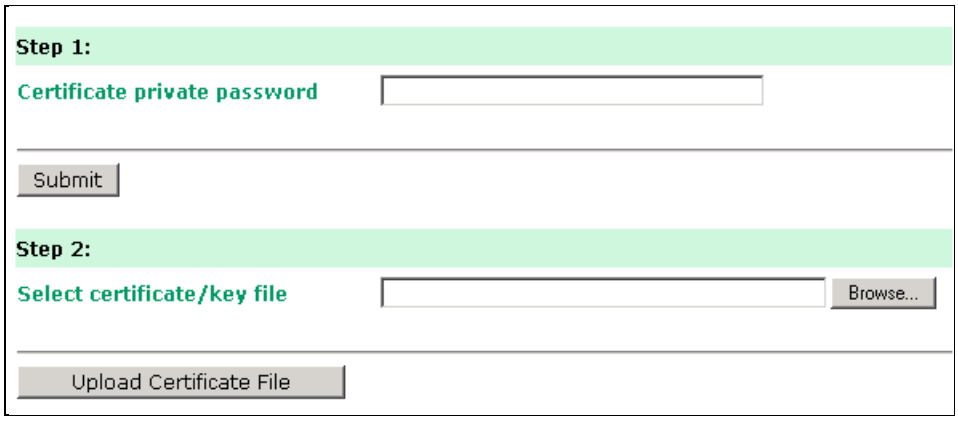
Certificate issued to: Shows the certificate user

Certificate issued by: Shows the certificate issuer

Certificate expiration date: Indicates when the certificate has expired

You can import a new WLAN certificate in ***Import WLAN Certificate*** by following these steps, in order:

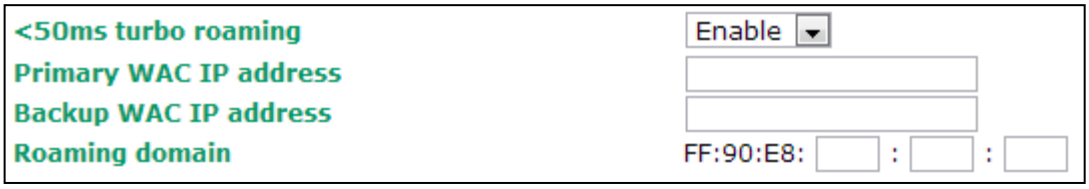
1. Input the corresponding password (or key) in the **Certificate private password** field and then click **Submit** to set the password.
2. The password will be displayed in the Certificate private password field. Click on the **Browse** button in ***Select certificate/key file*** and select the certificate file.
3. Click **Upload Certificate File** to import the certificate file. If the import succeeds, you can see the information uploaded in ***Current Certificate***. If it fails, you may need to return to step 1 to set the password correctly and then import the certificate file again.



NOTE The WLAN certificate will remain after the AWK-3121-RTG reboots. Even though it is expired, it can still be seen on the ***Current Certificate***.

WAC Settings

When <50ms turbo roaming is enabled, **Primary WAC IP address** , **Backup WAC IP address** and **Roaming domain** will be shown as follows.



Primary WAC IP address

Setting	Description	Factory Default
IP address	Enter the IP address of the primary WAC-1001 or WAC-2004	None

Backup WAC IP address

Setting	Description	Factory Default
IP address	Enter the IP address of the backup WAC-1001 or WAC-2004	None

Primary WAC IP address

Setting	Description	Factory Default
6 Hex characters	Specifies the area served by the WAC-1001 or WAC-2004. All related controllers, APs, and clients use this IP address as identification to work and communicate with each other	None

Advanced Settings

Several advanced functions are available to increase the functionality of your AWK-3121-RTG and wireless network system. A VLAN is a collection of clients and hosts grouped together as if they were connected to the broadcast domains in a layer 2 network. The DHCP server helps you deploy wireless clients efficiently. Packet filters provide security mechanisms, such as firewalls, in different network layers. Moreover, the AWK-3121-RTG can support SNMP to make network management easier.

VLAN Settings

Setting up Virtual LANs (VLANs) on your AWK series increases the efficiency of your network by dividing the LAN into logical segments, as opposed to physical segments. In general, VLANs are easier to manage.

The Virtual LAN (VLAN) Concept

What is a VLAN?

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch. Network reconfiguration can be done through software instead of physically relocating devices.

VLANs now extend as far as the reach of the access point signal. Clients can be segmented into wireless sub-networks via SSID and VLAN assignment. A Client can access the network by connecting to an AP configured to support its assigned SSID/VLAN.

Benefits of VLANs

VLANs are used to conveniently, efficiently, and easily manage your network in the following ways:

- Manage adds, moves, and changes from a single point of contact
- Define and monitor groups
- Reduce broadcast and multicast traffic to unnecessary destinations
- Improve network performance and reduce latency
- Increase security
- Secure network restricts members to resources on their own VLAN
- Clients roam without compromising security

VLAN Workgroups and Traffic Management

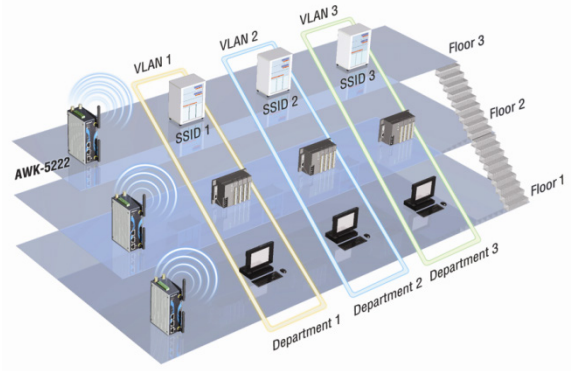
The AP assigns clients to a VLAN based on a Network Name (SSID). The AP can support up to 9 SSIDs per radio interface, with a unique VLAN configurable per SSID.

The AP matches packets transmitted or received to a network name with the associated VLAN. Traffic received by a VLAN is only sent on the wireless interface associated with that same VLAN. This eliminates unnecessary traffic on the wireless LAN, conserving bandwidth and maximizing throughput.

In addition to enhancing wireless traffic management, the VLAN-capable AP supports easy assignment of wireless users to workgroups. In a typical scenario, each user VLAN represents a department workgroup; for example, one VLAN could be used for a marketing department and the other for a human resource department.

In this scenario, the AP would assign every packet it accepted to a VLAN. Each packet would then be identified as marketing or human resource, depending on which wireless client received it. The AP would insert VLAN headers or "tags" with identifiers into the packets transmitted on the wired backbone to a network switch.

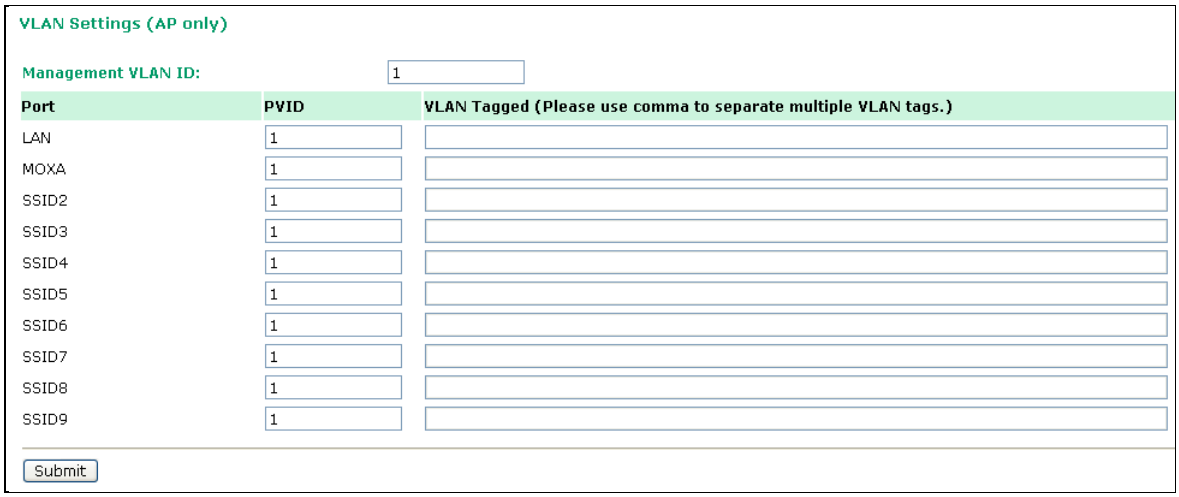
Finally, the switch would be configured to route packets from the marketing department to the appropriate corporate resources such as printers and servers. Packets from the human resource department could be restricted to a gateway that allowed access to only the Internet. A member of the human resource department could send and receive e-mail and access the Internet, but would be prevented from accessing servers or hosts on the local corporate network.



Configuring Virtual LAN

VLAN Settings

To configure the AWK's VLAN, use the VLAN Setting page to configure the ports.



Management VLAN ID

Setting	Description	Factory Default
VLAN ID ranges from 1 to 4094	Set the management VLAN of this AWK.	1

Port

Type	Description	Trunk Port
LAN	This port is the LAN port on the AWK.	Yes
WLAN	This is a wireless port for the specific SSID. This field will refer to the SSID that you have created. If more SSIDs have been created, new rows will be added.	

Port PVID

Setting	Description	Factory Default
VLAN ID ranging from 1 to 4094	Set the port's VLAN ID for devices that connect to the port. The port can be a LAN port or WLAN ports.	1

VLAN Tagged

Setting	Description	Factory Default
A comma-seperated list of VLAN IDs. Each of the VLAN IDs range from 1 to 4094.	Specify which VLANs can communicate with this specific VLAN.	(Empty)

NOTE The VLAN feature can allow wireless clients to manage the AP. If the VLAN Management ID matches a VLAN ID, then those wireless clients who are members of that VLAN will have AP management access.

CAUTION: Once a VLAN Management ID is configured and is equivalent to one of the VLAN IDs on the AP, all members of that User VLAN will have management access to the AP. Be careful to restrict VLAN membership to those with legitimate access to the AP.

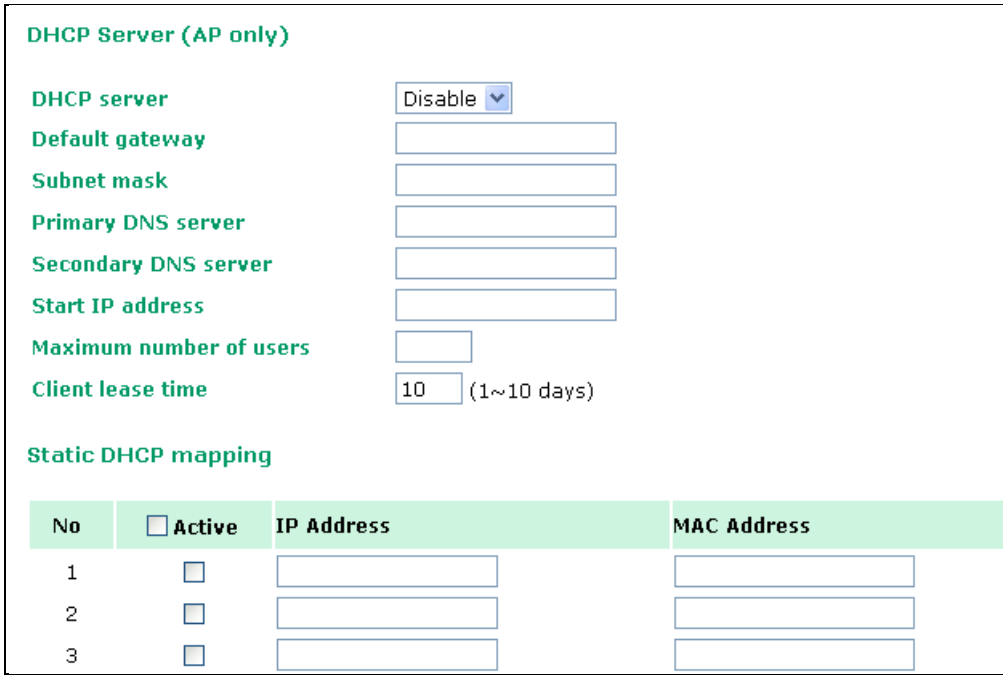
DHCP Server (For AP mode only)

DHCP (Dynamic Host Configuration Protocol) is a networking protocol that allows administrators to assign temporary IP addresses to network computers by "leasing" an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

The AWK-3121-RTG can act as a simplified DHCP server and easily assign IP addresses to your wireless clients by responding to the DHCP requests from the client ends. The IP-related parameters you set on this page will also be sent to the client.

You can also assign a static IP address to a specific client by entering its MAC address. The AWK-3121-RTG provides a **Static DHCP mapping** list with up to 16 entities. Be reminded to check the **Active** check box for each entity to activate the setting.

You can check the IP assignment status under **Status → DHCP Client List**.



DHCP server

Setting	Description	Factory Default
Enable	Enables AWK-3121-RTG as a DHCP server	Disable
Disable	Disable DHCP server function	

Default gateway

Setting	Description	Factory Default
IP address of a default gateway	The IP address of the router that connects to an outside network	None

Subnet mask

Setting	Description	Factory Default
subnet mask	Identifies the type of sub-network (e.g., 255.255.0.0 for a Class B network, or 255.255.255.0 for a Class C network)	None

Primary/ Secondary DNS server

Setting	Description	Factory Default
IP address of Primary/ Secondary DNS server	The IP address of the DNS Server used by your network. After entering the DNS Server's IP address, you can use URL as well. The Secondary DNS server will be used if the Primary DNS server fails to connect.	None

Start IP address

Setting	Description	Factory Default
IP address	Indicates the IP address which AWK-3121-RTG can start assigning	None

Maximum number of users

Setting	Description	Factory Default
1 – 999	Specifies how many IP address can be assigned continuously	None

Client lease time

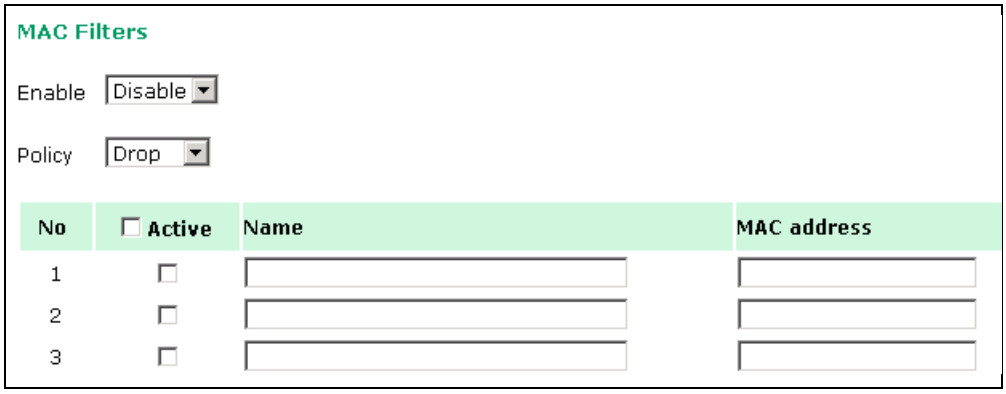
Setting	Description	Factory Default
1 – 10 days	The lease time for which an IP address is assigned. The IP address may go expired after the lease time is reached.	10 (days)

Packet Filters

The AWK-3121-RTG includes various filters for **IP-based** packets going through LAN and WLAN interfaces. You can set these filters as a firewall to help enhance network security.

MAC Filter

The AWK-3121-RTG's MAC filter is a policy-based filter that can allow or filter out IP-based packets with specified MAC addresses. The AWK-3121-RTG provides 8 entities for setting MAC addresses in your filtering policy. Remember to check the **Active** check box for each entity to activate the setting.



Enable

Setting	Description	Factory Default
Enable	Enables MAC filter	Disable
Disable	Disables MAC filter	

Policy

Setting	Description	Factory Default
Accept	Only the packets fitting the entities on list can be allowed.	Drop
Drop	Any packet fitting the entities on list will be denied.	

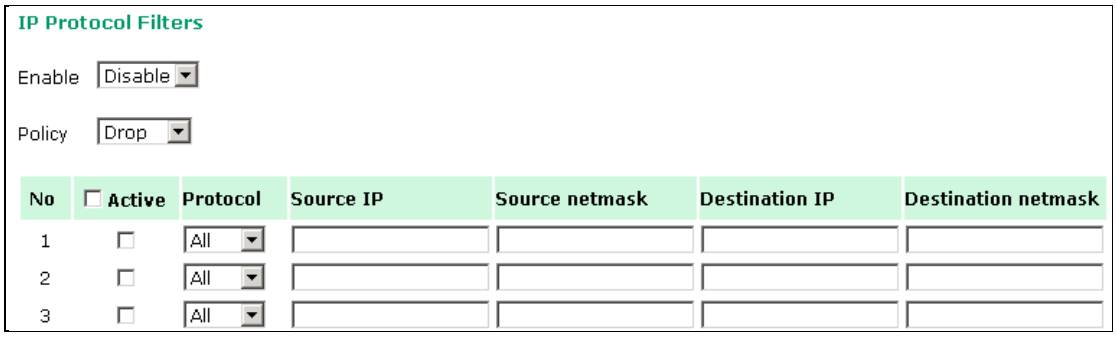
ATTENTION

Be careful when you enable the filter function:
Drop + "no entity on list is activated" = all packets are **allowed**
Accept + "no entity on list is activated" = all packets are **denied**

IP Protocol Filter

The AWK-3121-RTG's IP protocol filter is a policy-based filter that can allow or filter out IP-based packets with specified IP protocol and source/destination IP addresses.

The AWK-3121-RTG provides 8 entities for setting IP protocol and source/destination IP addresses in your filtering policy. Four IP protocols are available: **All**, **ICMP**, **TCP**, and **UDP**. You must specify either the Source IP or the Destination IP. By combining IP addresses and netmasks, you can specify a single IP address or a range of IP addresses to accept or drop. For example, "IP address 192.168.1.1 and netmask 255.255.255.255" refers to the sole IP address 192.168.1.1. "IP address 192.168.1.1 and netmask 255.255.255.0" refers to the range of IP addresses from 192.168.1.1 to 192.168.255. Remember to check the **Active** check box for each entity to activate the setting.



Enable

Setting	Description	Factory Default
Enable	Enables IP protocol filter	Disable
Disable	Disables IP protocol filter	

Policy

Setting	Description	Factory Default
Accept	Only the packets fitting the entities on the list can be allowed	Drop
Drop	Any packet fitting the entities on the list will be denied	

ATTENTION

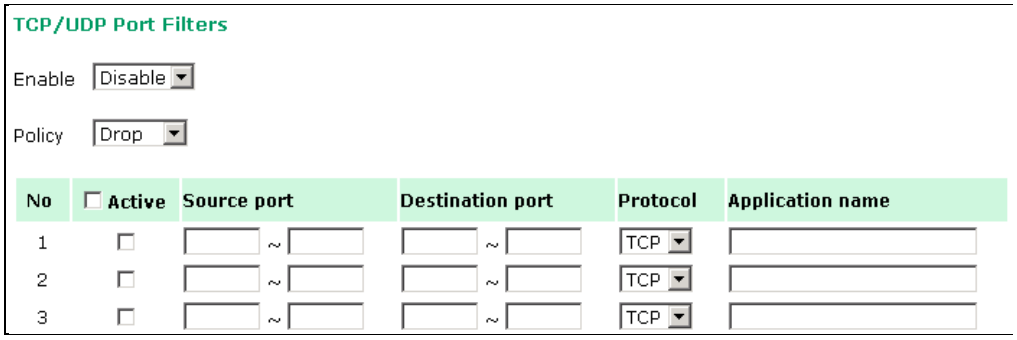
Be careful when you enable the filter function:
Drop + "no entity on list is activated" = all packets are **allowed.**
Accept + "no entity on list is activated" = all packets are **denied.**

TCP/UDP Port Filter

The AWK-3121-RTG's TCP/UDP port filter is a policy-based filter that can allow or filter out TCP/UDP-based packets with a specified source or destination port.

The AWK-3121-RTG provides 8 entities for setting the range of source/destination ports of a specific protocol. In addition to selecting TCP or UDP protocol, you can set either the source port, destination port, or both. The end port can be left empty if only a single port is specified. Of course, the end port cannot be larger then the start port.

The **Application name** is a text string that describes the corresponding entity with up to 31 characters. Remember to check the **Active** check box for each entity to activate the setting.



Enable

Setting	Description	Factory Default
Enable	Enables TCP/UDP port filter	Disable
Disable	Disables TCP/UDP port filter	

Policy

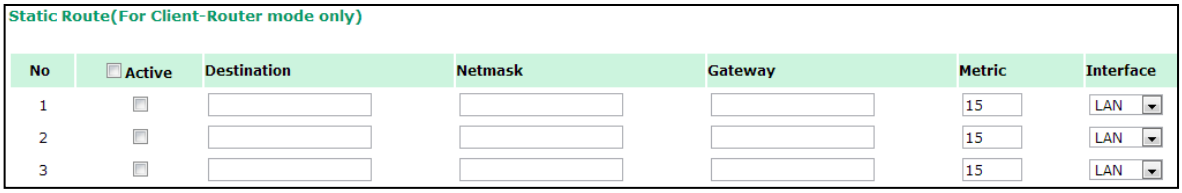
Setting	Description	Factory Default
Accept	Only the packets fitting the entities on list can be allowed.	Drop
Drop	Any packet fitting the entities on list will be denied.	

ATTENTION

Be careful when you enable the filter function:
Drop + "no entity on list is activated" = all packets are **allowed**
Accept + "no entity on list is activated" = all packets are **denied**

Static Route (For Client-Router mode only)

The Static Routing page is used to configure AWK-3121-RTG's static routing table.



Active

Click the checkbox to enable Static Routing.

Destination

You can specify the destination IP address.

Netmask

This option is used to specify the subnet mask for this IP address.

Gateway

The IP address of the router that connects the LAN to an outside network.

Metric

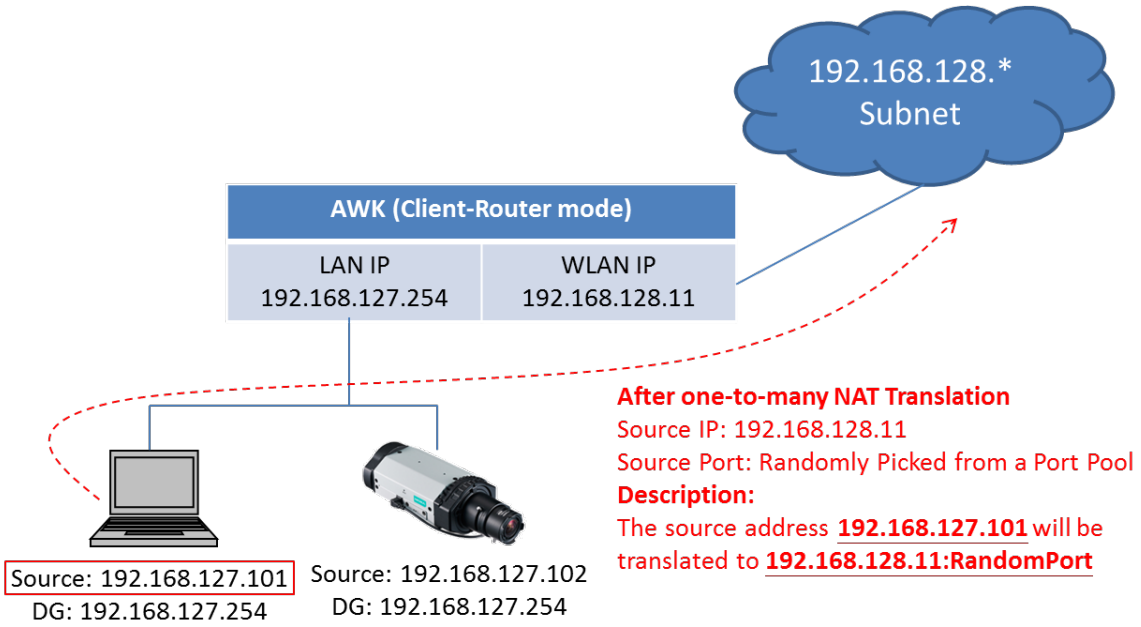
Use this option to specify a "cost" for accessing the neighboring network.

Interface

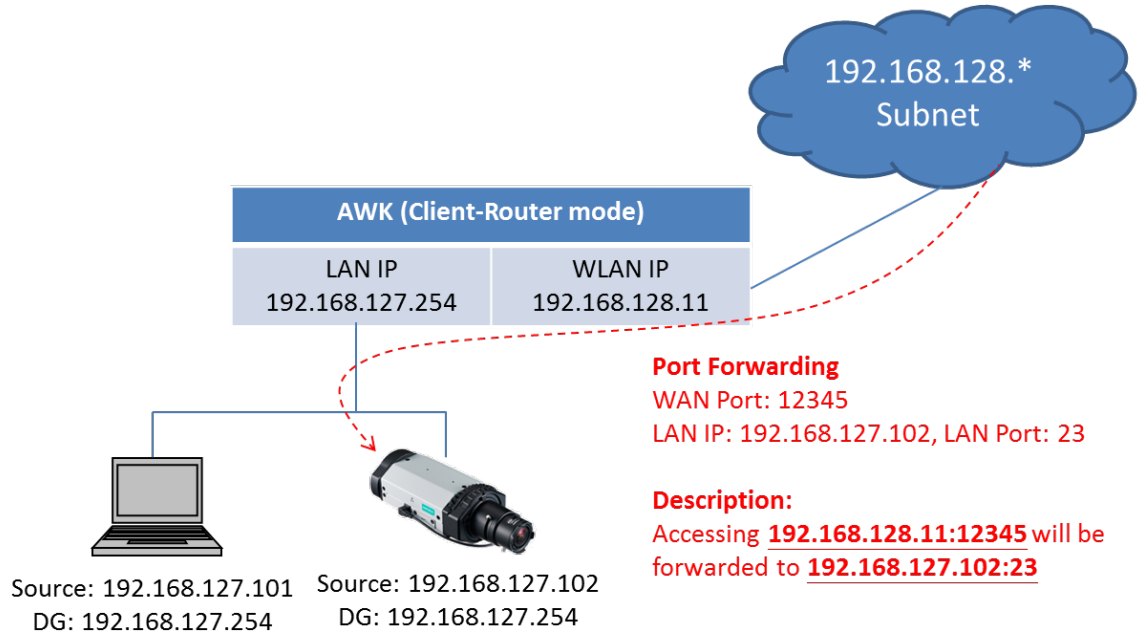
You can select which interface does your routing rules would be set.

NAT Settings/Port Forwarding (For Client-Router mode only)

Network Address Translation (NAT)—or more specifically, one-to-many NAT, NAPT, or PAT—is supported to facilitate the Client-Router operation mode. This features translates the out-going communication from multiple private IPs to a single external IP (WLAN IP) with randomly assigned port for return traffic.

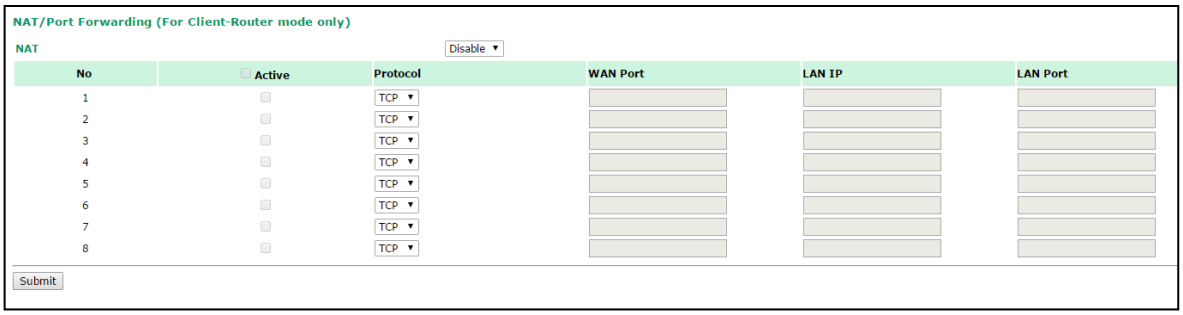


Port Forwarding is needed to allow external devices to initiate communication. Port Forwarding specifies a static map between external ports (WAN Port) and internal IP/port combos (LAN IP/LAN Port)



Enabling NAT and Port Forwarding provides the following benefits:

- Uses the NAT function to hide the Internal IP address of a critical network or device to increase the level of security of industrial network applications.
- Uses the same private IP address for different, but identical, groups of Ethernet devices. For example, 1-to-1 NAT makes it easy to duplicate or extend identical production lines



NAT

Setting	Description	Factory Default
Enable/Disable	Enables or disables the NAT translation	Disable

Port Forwarding

Active: Click the checkbox to enable Port Forwarding rule(s).
Protocol: Specifies the communication protocol.
WAN Port: Specifies the external port to be forwarded to.
LAN IP: Specifies the "forward to" LAN IP.
LAN Port: Specifies the "forward to" LAN Port.

SNMP Agent

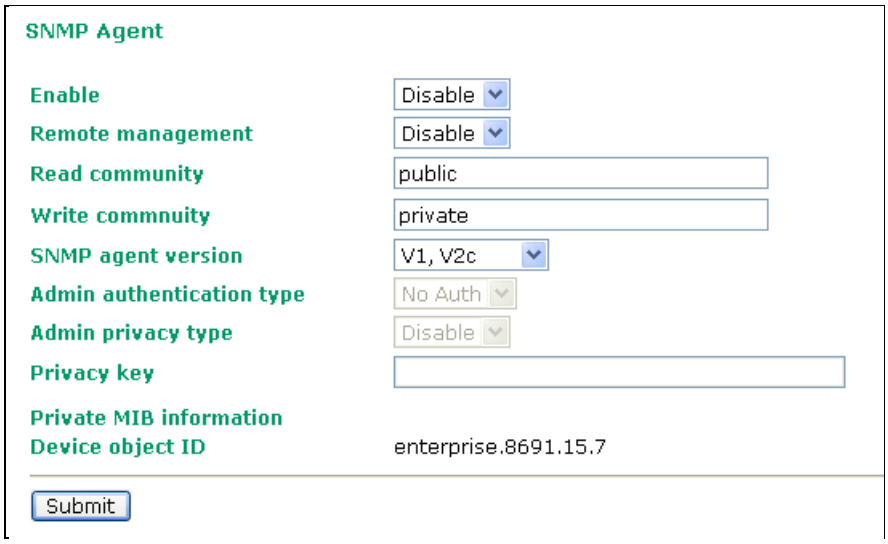
The AWK-3121-RTG supports SNMP V1/V2c/V3. SNMP V1 and SNMP V2c use a community string match for authentication, which means that SNMP servers access all objects with read-only or read/write permissions using the community string *public*/*private* (default value). SNMP V3, which requires you to select an authentication level of MD5 or SHA, is the most secure protocol. You can also enable data encryption to enhance data security.

The AWK-3121-RTG's MIB can be found in the software CD and supports reading the attributes via SNMP. (Only ***get*** method is supported.)

SNMP security modes and security levels supported by the AWK-3121-RTG are shown in the following table. Select the security mode and level that will be used to communicate between the SNMP agent and manager.

Protocol Version	Setting on UI web page	Authentication Type	Data Encryption	Method
SNMP V1, V2c	V1, V2c Read Community	Community string	No	Use a community string match for authentication
	V1, V2c Write/Read Community	Community string	No	Use a community string match for authentication
SNMP V3	No-Auth	No	No	Use account with admin or user to access objects
	MD5 or SHA	Authentication based on MD5 or SHA	No	Provides authentication based on HMAC-MD5, or HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.
	MD5 or SHA	Authentication based on MD5 or SHA	Data encryption key	Provides authentication based on HMAC-MD5 or HMAC-SHA algorithms, and data encryption key. 8-character passwords and a data encryption key are the minimum requirements for authentication and encryption.

The following parameters can be configured on the **SNMP Agent** page. A more detailed explanation of each parameter is given below the following figure.



Enable

Setting	Description	Factory Default
Enable	Enables SNMP Agent	Disable
Disable	Disables SNMP Agent	

Remote Management

Setting	Description	Factory Default
Enable	Allow remote management via SNMP agent	Disable
Disable	Disallow remote management via SNMP agent	

Read community (for V1, V2c)

Setting	Description	Factory Default
V1, V2c, V3 Read Community	Use a community string match with a maximum of 31 characters for authentication. This means that the SNMP agent can access all objects with read-only permissions using this community string.	public

Write community (for V1, V2c)

Setting	Description	Factory Default
V1, V2c Read /Write Community	Use a community string match with a maximum of 31 characters for authentication. This means that the SNMP agent can accesses all objects with read/write permissions using this community string.	private

SNMP agent version

Setting	Description	Factory Default
V1, V2c, V3, or V1, V2c, or V3 only	Select the SNMP protocol version used to manage the switch.	V1, V2c

Admin auth type (for V1, V2c, V3, and V3 only)

Setting	Description	Factory Default
No Auth	Use admin account to access objects. No authentication	No Auth
MD5	Provide authentication based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication.	
SHA	Provides authentication based on HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.	

Admin private key (for V1, V2c, V3, and V3 only)

Setting	Description	Factory Default
Disable	No data encryption	Disable
DES	DES-based data encryption	
AES	AES-based data encryption	

Private key

A data encryption key is the minimum requirement for data encryption (maximum of 63 characters)

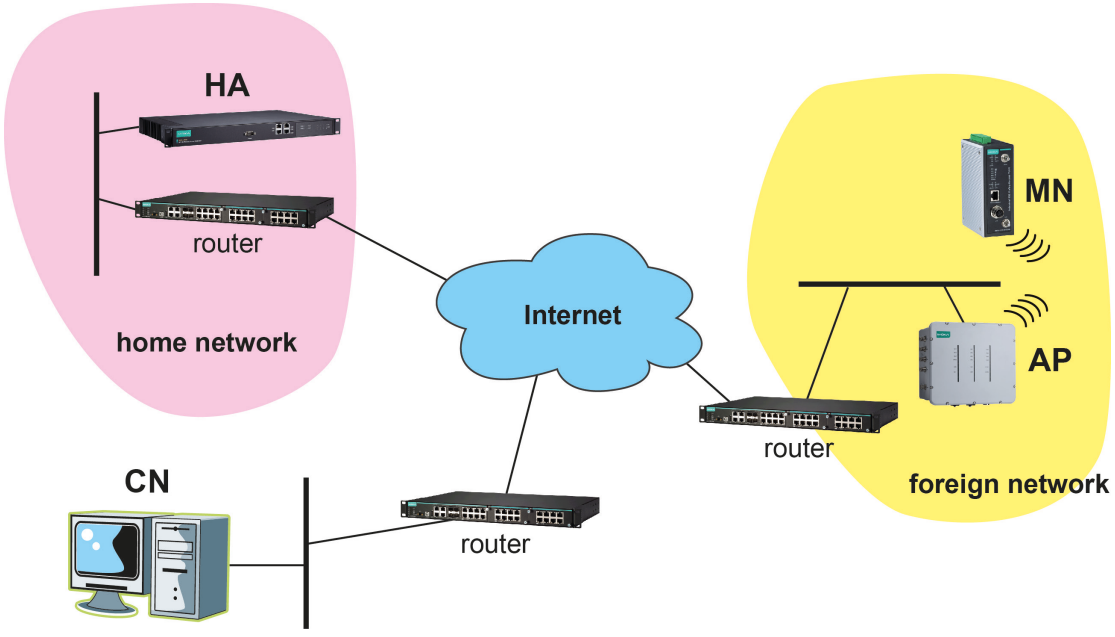
Private MIB Information Device Object ID

Also known as ***OID***. This is the AWK-3121-RTG's enterprise value. It is fixed.

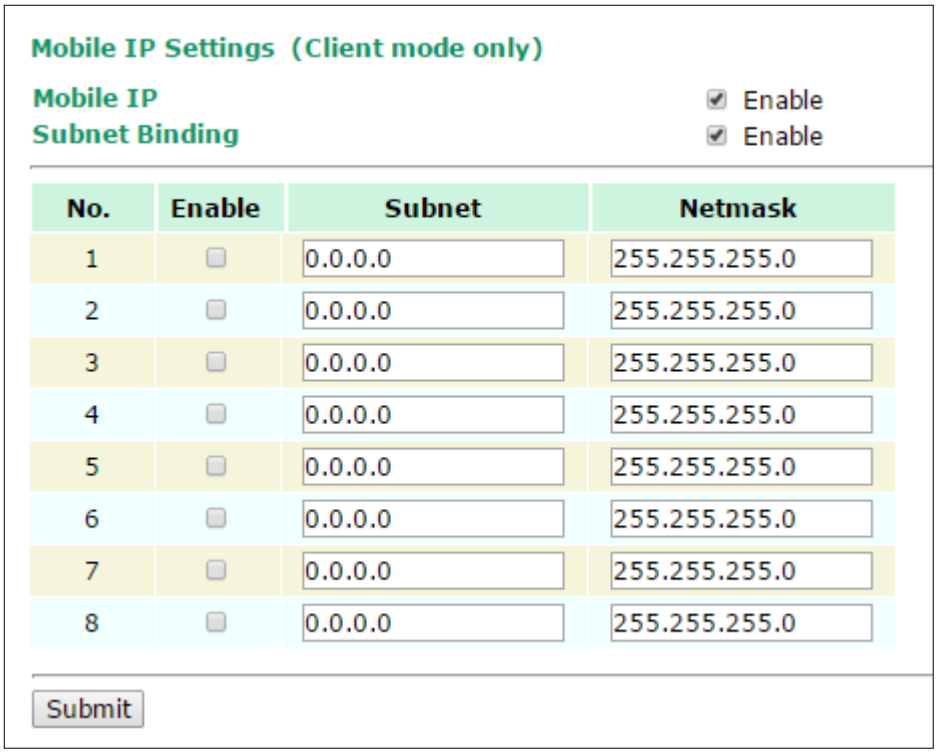
Mobile IP Settings

The mobile IP technology enables the AWK-3121-RTG to roam between Layer 3 networks with a roaming break time less than 50 ms. When the AWK-3121-RTG is in client/client router mode, it is a mobile node (MN) that is able to roam across different subnets without changing its IP address.

Mobile IP Topology Example:



Terminology	Description
Mobile Node (MN)	A host or router that changes its location from one network to another.
Home network	The network within which the MN receives its identifying IP address (home address)
Home address	The IP address assigned to the MN within its home network
Foreign network	The network in which an MN is operating when away from its home network
Home agent (HA)	A router on the home network that provides services to the MN. The home agent intercepts packets sent to the MN within the home network, encapsulates them, and then tunnels them to the MN.
Correspondent Node (CN)	A peer with which a mobile node is communicating
Co-located Care-of Address (CCoA)	The new IP address of the MN when operating on a foreign network.
Binding	The association of the home address with a CCoA



Setting	Description	Factory Default
Mobile IP	Enable/disable mobile IP capability of the client (mobile node) for L3 controller based roaming	Disable
Subnet Binding	Define a subnet of devices connected behind the client (MN) so that data will be forwarded to the corresponding device subnets. Proper IP planning is required to avoid configuring the subnet binding IP to limit access to the AWK.	Disable

Note that when the Mobile IP is enabled, the corresponding AP and WAC (HA) controller will also need to be configured properly (with 50 ms roaming enabled) to ensure correct operation of the L3 roaming network.

Auto Warning Settings

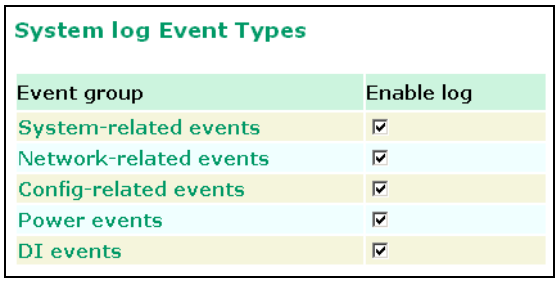
Since industrial-grade devices are often located at the endpoints of a system, these devices will not always know what is happening elsewhere on the network. This means that these devices, including wireless APs or clients, must provide system maintainers with real-time alarm messages. Even when system administrators are out of the control room for an extended period, they can still be informed of the status of devices almost instantaneously when exceptions occur.

In addition to logging these events, the AWK-3121-RTG supports different approaches to warn engineers automatically, such as SNMP trap, e-mail, and relay output. It also supports two digital inputs to integrate sensors into your system to automate alarms by email and relay output.

System Log

System Log Event Types

Detail information for grouped events is shown in the following table. You can check the box for Enable log to enable the grouped events. All default values are enabled (checked). The log for system events can be seen in Status → System Log.



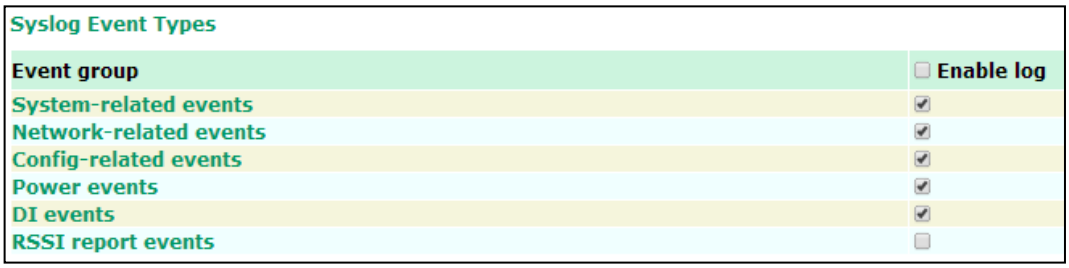
System-related events	**Event is triggered when…**
System restart (warm start)	The AWK-3121-RTG is rebooted, such as when its settings are changed (IP address, subnet mask, etc.).
Network-related events	**Event is triggered when…**
LAN link on	The LAN port is connected to a device or network.
LAN link off	The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down).
Client joined/ left (for AP mode)	A wireless client is associated or disassociated.
WLAN connected to AP (for Client/ Client-Router mode)	The AWK-3121-RTG is associated with an AP.
WLAN disconnected (for Client/ Client-Router mode)	The AWK-3121-RTG is disassociated from an AP.
Config-related events	**Event is triggered when…**
Configuration Changed	A configuration item has been changed.
Configuration file import via Web Console	The configuration file is imported to the AWK-3121-RTG.
Console authentication failure	An incorrect password is entered.
Firmware upgraded	The AWK-3121-RTG's firmware is updated.
Power events	**Event is triggered when…**
Power 1/2 transition (On -> Off)	The AWK-3121-RTG is powered down in PWR1/2.
PoE transition (On -> Off)	The AWK-3121-RTG is powered down in PoE.
Power 1/2 transition (Off -> On)	The AWK-3121-RTG is powered via PWR1/2.
PoE transition (Off -> On)	The AWK-3121-RTG is powered via PoE.
DI events	**Event is triggered when…**
DI1/2 transition (On -> Off)	Digital Input 1/2 is triggered by on to off transition
DI1/2 transition (Off -> On)	Digital Input 1/2 is triggered by off to on transition

Syslog

This function provides the event logs for the Syslog server. The function supports up to three configurable Syslog servers and Syslog server UDP port numbers. When an event occurs, the event will be sent as a Syslog UDP packet to the specified Syslog servers.

Syslog Event Types

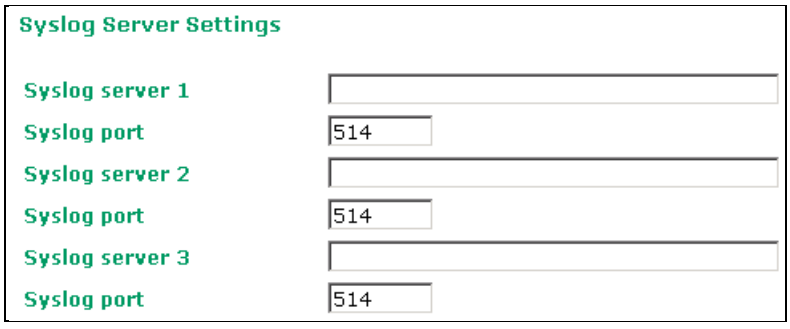
Detail information for the grouped events is shown in the following table. You can check the box for **Enable log** to enable the grouped events. All default values are enabled (checked). Details for each event group can be found on the "System log Event Types" table on page 3-33.



NOTE **RSSI report events (Only for Client and Client-Router mode)** is good for site survey stage and need to use special Utility to draw RSSI as a table. But this function would make extra traffic load, we recommend **disable** this function in normal using.

Syslog Server Settings

You can configure the parameters for your Syslog servers in this page.



Syslog server 1/ 2/ 3

Setting	Description	Factory Default
IP address	Enter the IP address of the 1st/ 2nd/ 3rd Syslog Server	None

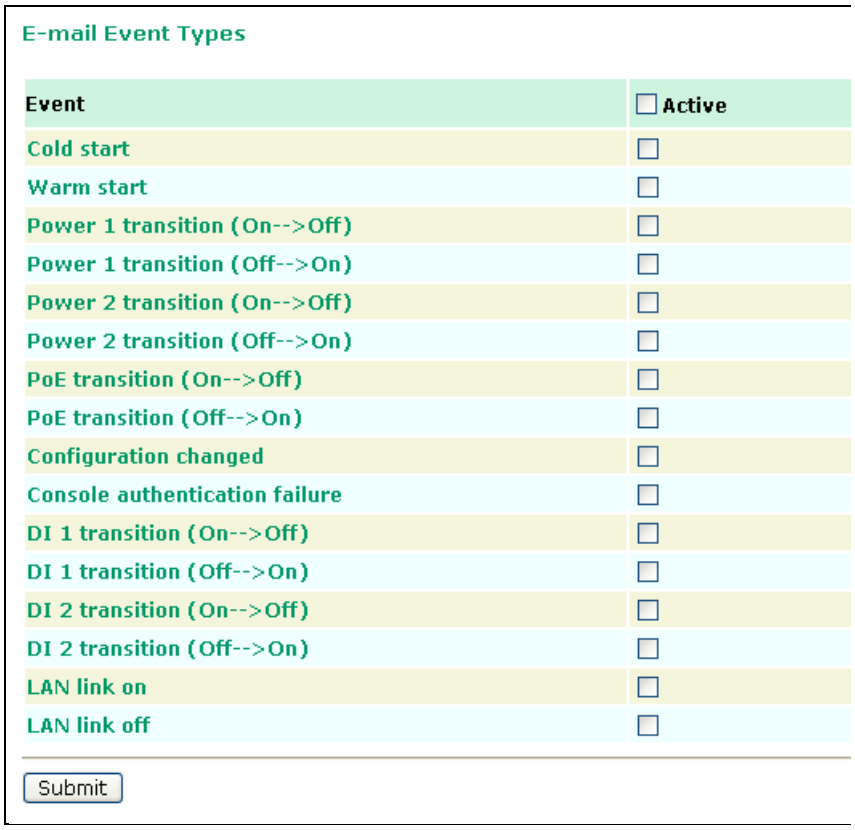
Syslog port

Setting	Description	Factory Default
Port destination (1 to 65535)	Enter the UDP port of the corresponding Syslog server	514

E-mail

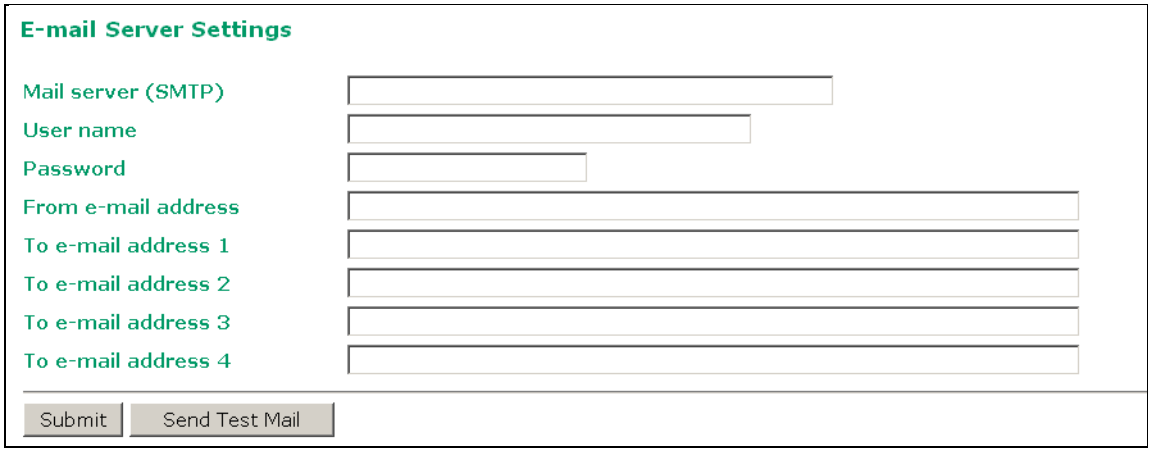
E-mail Event Types

Check the box for **Active** to enable the event items. All default values are deactivated (unchecked). Details for each event item can be found on the "System log Event Types" table on page 3-31.



E-mail Server Settings

You can set up to 4 e-mail addresses to receive alarm emails from the AWK-3121-RTG. The following parameters can be configured on the **E-mail Server Settings** page. In addition, a **Send Test Mail** button can be used to test whether the Mail server and e-mail addresses work well. More detailed explanations about these parameters are given after the following figure.



Mail server (SMTP)

Setting	Description	Factory Default
IP address	The IP Address of your email server.	None

User name & Password

Setting	Description	Factory Default
	User name and password used in the SMTP server	None

From e-mail address

Setting	Description	Factory Default
Max. 63 characters	Enter the administrator's e-mail address which will be shown in the "From" field of a warning e-mail.	None

To E-mail address 1/ 2/ 3/ 4

Setting	Description	Factory Default
Max. 63 characters	Enter the receivers' e-mail addresses.	None

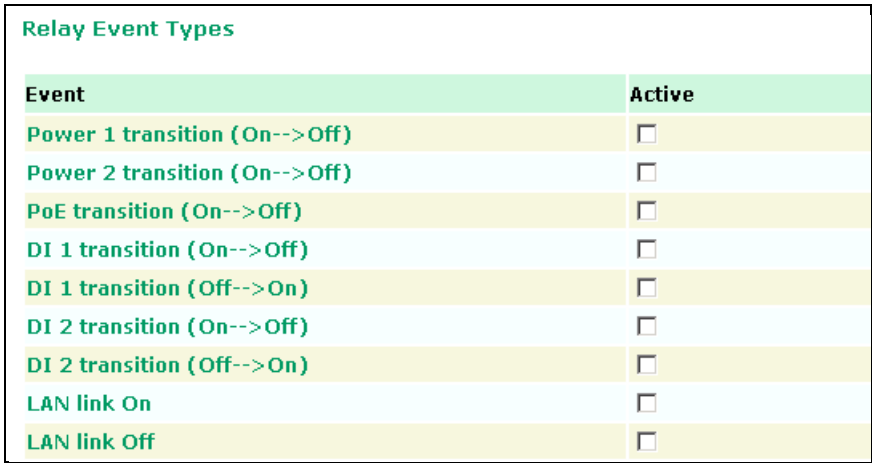
Relay

The AWK-3121-RTG has one relay output, which consists of 2 terminal block contacts on the AWK-3121-RTG's top panel. These relay contacts are used to indicate user-configured events and system failure.

The two wires attached to the relay contacts form an open circuit when a user-configured event is triggered. If a user-configured event does not occur, the relay circuit will remain closed. For safety reasons, the relay circuit is kept open when the AWK-3121-RTG is not powered.

Relay Event Types

You can check the box for **Active** to enable the event items. All default values are deactivated . Details for each event item can be found in the "System log Event Types" table on page 3-33.

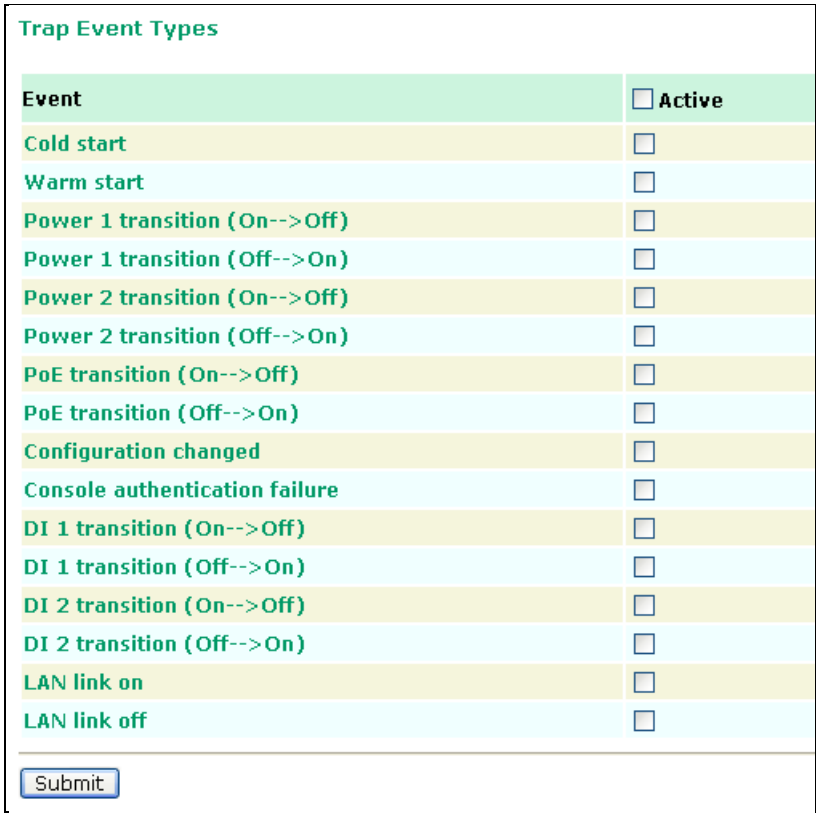


Trap

Traps can be used to signal abnormal conditions (notifications) to a management station. This trap-driven notification can make your network more efficient.

Because a management station usually takes care of a large number of devices that have a large number of objects, it will be overloading for the management station to poll or send requests to query every object on every device. It would be better if the managed device agent could notify the management station by sending a message known as a trap for the event.

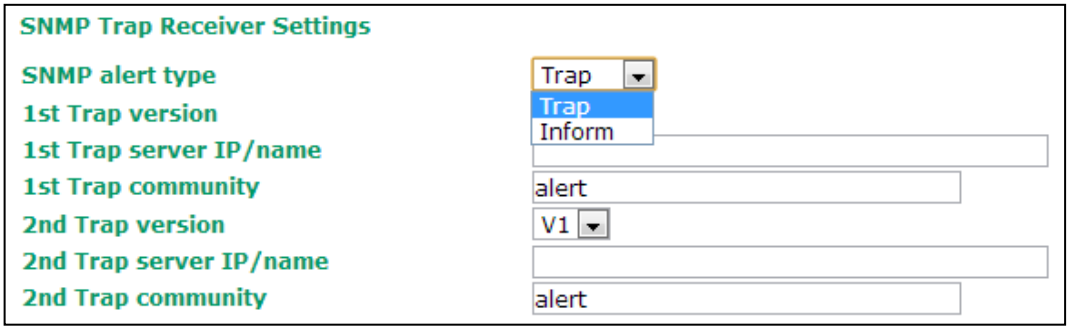
Trap Event Types



SNMP Trap Receiver Settings

In SNMP traps mode, Traps are defined in SMIv1 MIBs (SNMPv1) and SMIv2 MIBs (SNMPv2c). The two styles are basically equivalent, and it is possible to convert between the two. You can set the parameters for SNMP trap receivers through the web page.

In SNMP Inform mode, SNMPv2 provides an inform mechanism. When an inform message is sent from the SNMP agent to the NMS, the receiver sends a response to the sender acknowledging receipt of the event. This behavior is similar to that of the get and set request. If the SNMP agent doesn't receive a response from the NMS for a period of time, the agent will resend the trap to the NMS agent.



1st / 2nd Trap version (Only for Trap mode)

Setting	Description	Factory Default
V1	SNMP trap defined in SNMPv1	V1
V2	SNMP trap defined in SNMPv2	

1st / 2nd Trap server IP/name

Setting	Description	Factory Default
IP address or host name	Enter the IP address or name of the trap server used by your network.	None

1st / 2nd Trap community

Setting	Description	Factory Default
Max. of 31 characters	Use a community string match with a maximum of 31 characters for authentication.	alert

Status

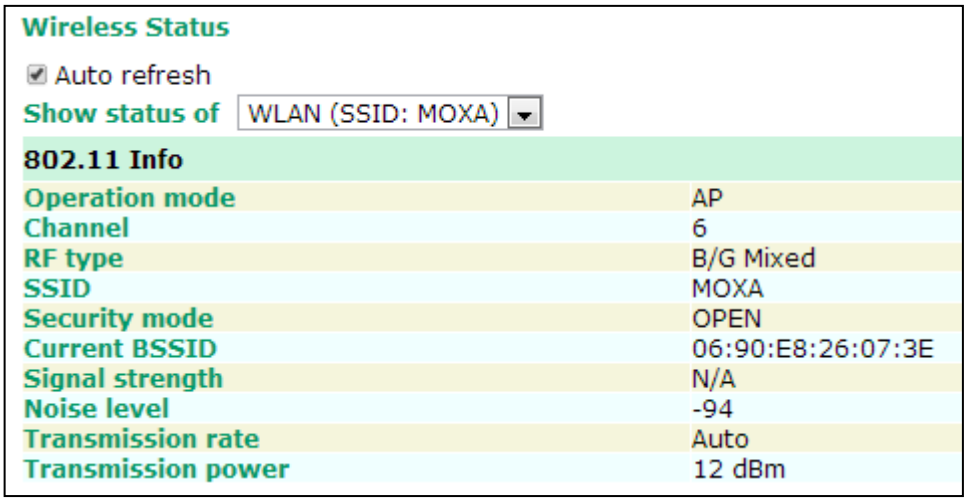
Wireless Status

The status for **802.11 info** parameters, such as Operation mode and Channel, are shown on the **Wireless Status** page. The status will refresh every 5 seconds if the **Auto refresh** box is checked.

Certain values for **802.11 info** may not show up due to different operation modes. As a result, **Current BSSID** and **Signal strength** are not available in AP mode.

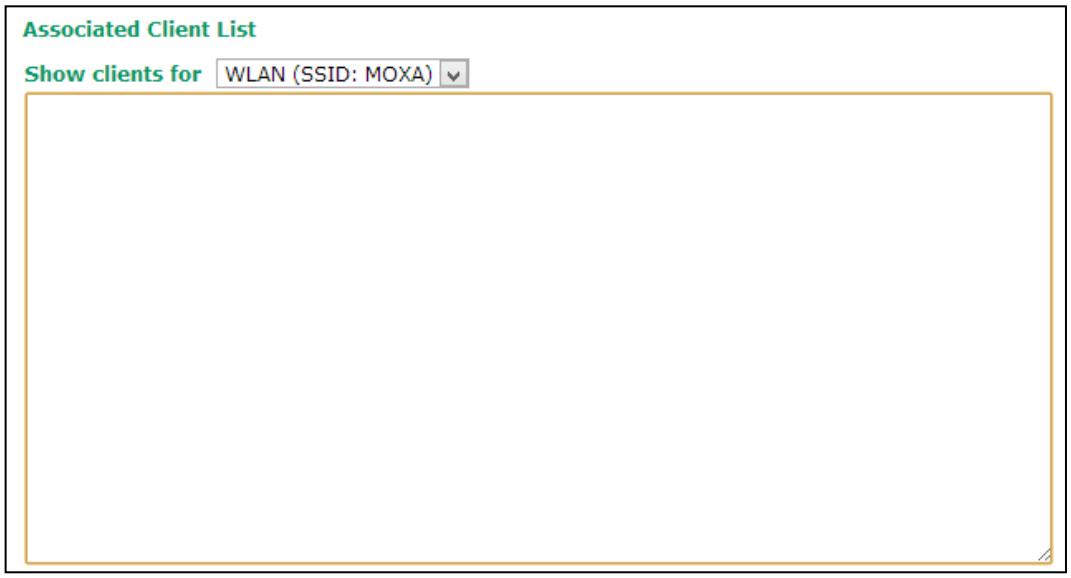
It is helpful to use the continuously updated information on this page, such as **Signal strength**, to monitor the signal strength of the AWK-3121-RTG in Client mode.

The transmission power indicated is the current transmission power being updated periodically.



Associated Client List (for AP mode only)

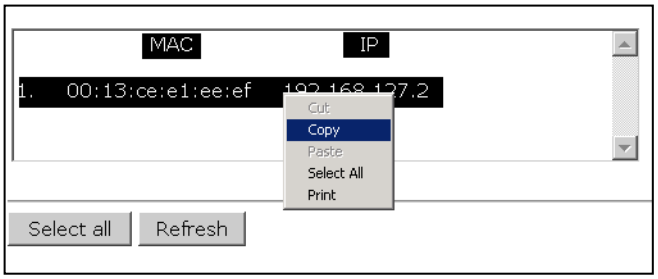
Associated Client List shows all the clients that are currently associated to a particular AWK-3121-RTG. You can click **Select all** to select all the content in the list for further editing. You can click **Refresh** to refresh the list.



DHCP Client List (for AP mode only)

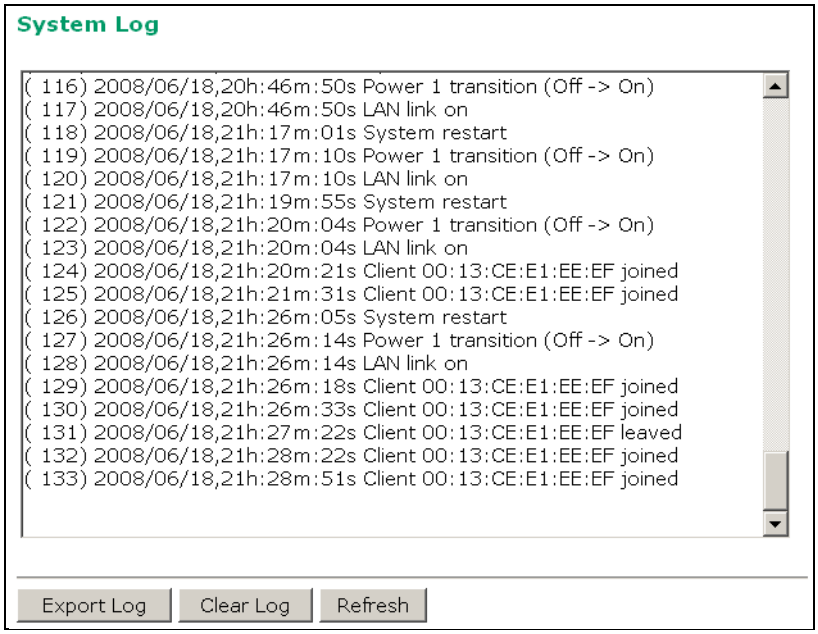
The DHCP Client List shows all the clients that require and have successfully received IP assignments. You can click the **Refresh** button to refresh the list.

You can press **Select all** button to select all content in the list for further editing.



System Log

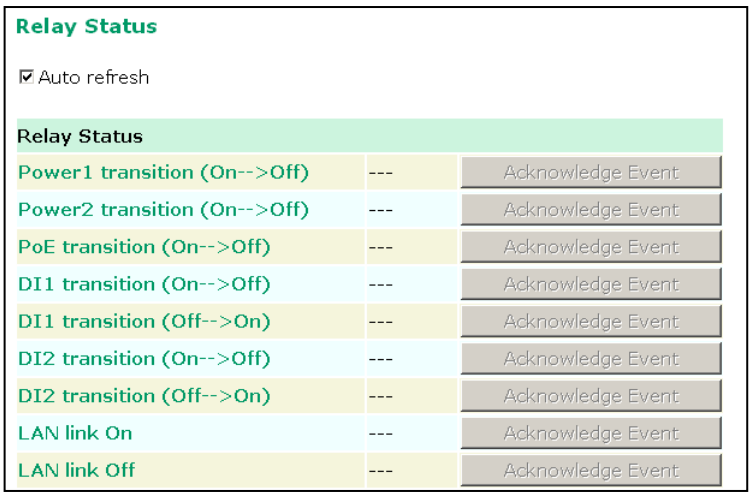
Triggered events are recorded in System Log. You can export the log contents to an available viewer by clicking **Export Log**. You can use the **Clear Log** button to clear the log contents and the **Refresh** button to refresh the log.



Relay Status

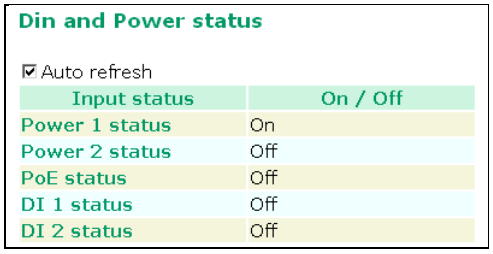
The status of user-configurable events can be found under **Relay Status**. The status will refresh every 5 seconds if the **Auto refresh** box is checked.

If an event is triggered, it will be noted on this list. System administrators can click **Acknowledge Event** when he has acknowledged the event and addressed it.



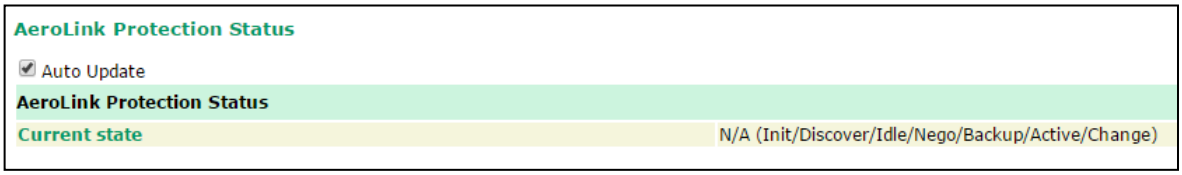
DI and Power Status

The status of power inputs and digital inputs is shown on this web page. The status will refresh every 5 seconds if the **Auto refresh** box is checked.



AeroLink Protection Status (For Client/Slave mode only)

After enabling AeroLink Protection from the Advanced WLAN Setup panel, the following table shows the current state of the AeroLink Protection for easier diagnosis.

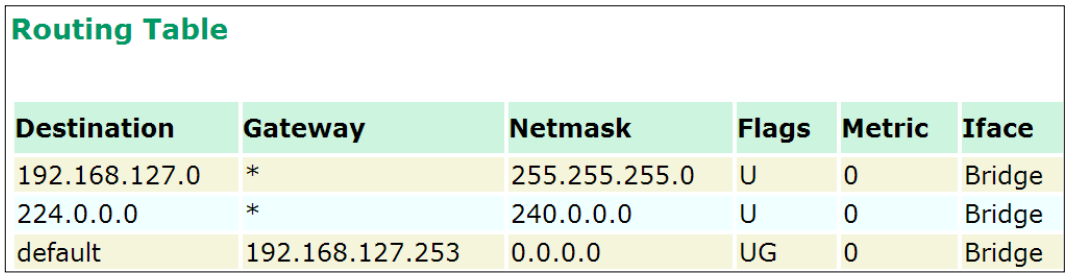


An AeroLink Protection member could be in 1 or 7 different states:

Initiation State (Init): Initiates the AeroLink Protection Protocol.
Discovering State (Discover): Discovers other AeroLink Protection members for further negotiation.
Idle State (Idle): Internal protocol checkpoint.
Negotiation State (Nego): Negotiates with other AeroLink Protection members and selects Active node.
Backup State (Backup): After negotiation, this node is assigned as the Backup node. All traffic will pass through the Active node. NOTE: When a node is acting as a Backup node, the STATE LED for the node will blink to advertise this fact to nearby support engineers.
Active State (Active): After negotiation, this node is assigned Active node status, which means that all traffic will pass through that node.
Role Change State (Change): If the Active node is no longer capable of data transmission via the WLAN, the device will enter "change state," which will result in the device going back to Nego state (likely becoming the Backup device since the active link is down).

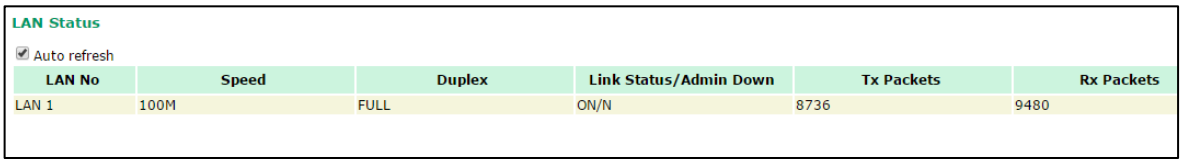
Routing Table

The Routing Table page shows all routing entries.



LAN Status

The LAN Status page displays LAN port status information, including speed, duplex status, on/off status, as well as the number of packets transmitted and received.

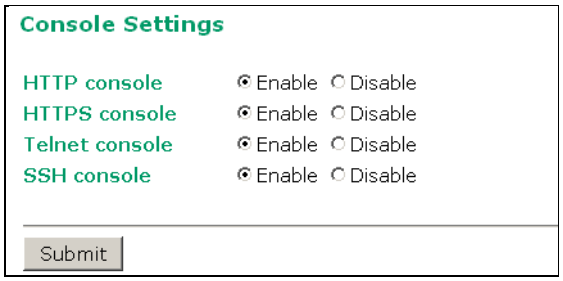


Maintenance

Maintenance functions provide the administrator with tools to manage the AWK-3121-RTG and wired/wireless networks.

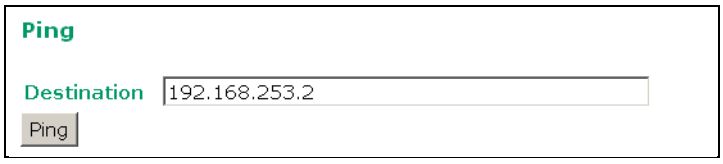
Console Settings

You can enable or disable access permission for the following consoles: HTTP, HTTPS, Telnet and SSH connections. For more security, we recommend you only allow access to the two secured consoles, HTTPS and SSH.

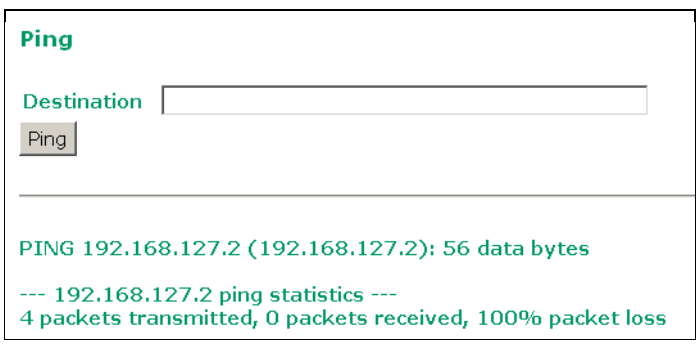


Ping

Ping helps to diagnose the integrity of wired or wireless networks. By inputting a node's IP address in the **Destination** field, you can use the **ping** command to make sure it exists and whether or not the access path is available.



If the node and access path are available, you will see that all packets were successfully transmitted with no loss. Otherwise, some, or even all, packets may get lost, as shown in the following figure.

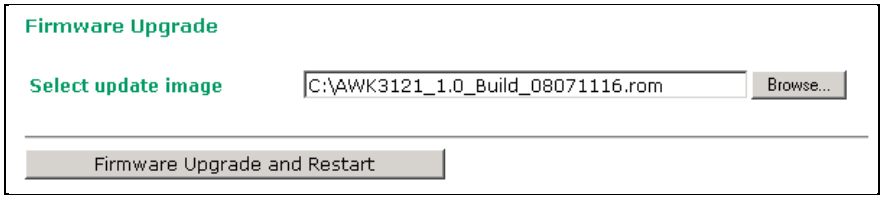


Firmware Upgrade

The AWK-3121-RTG can be enhanced with more value-added functions by installing firmware upgrades. The latest firmware is available at Moxa's download center.

Before running a firmware upgrade, make sure the AWK-3121-RTG is off-line. Click the **Browse** button to specify the firmware image file and click **Firmware Upgrade and Restart** to start the firmware upgrade. After the progress bar reaches 100%, the AWK-3121-RTG will reboot itself.

When upgrading your firmware, the AWK-3121-RTG's other functions are forbidden.



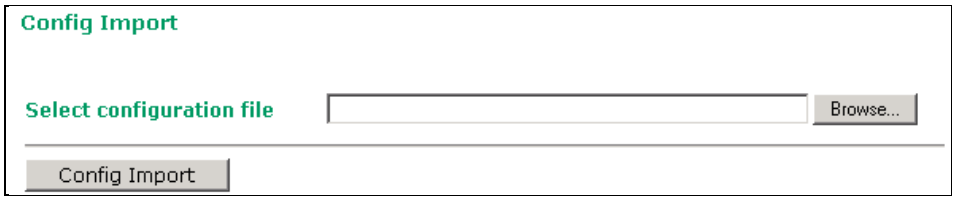
ATTENTION

Please make sure the power source is stable when you upgrade your firmware. An unexpected power breakup may damage your AWK-3121-RTG.

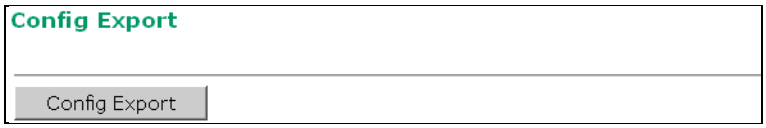
Config Import Export

First way you can back up or restore the AWK-3121-RTG's configuration with **Config Import Export**.

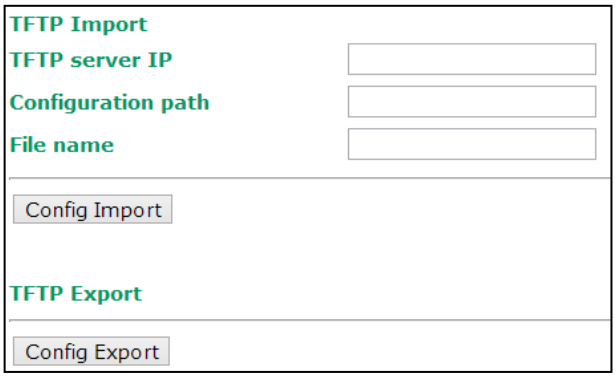
In the **Config Import** section, click **Browse** to specify the configuration file and click **Config Import** button to begin importing the configuration.



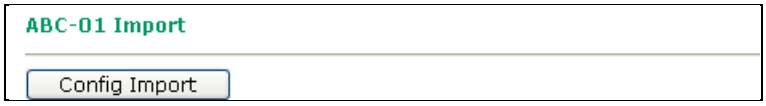
In the **Config Export** section, click the **Config Export** button and save the configuration file onto your local storage media. The configuration file is a text file and you can view and edit it with a general text-editing tool.

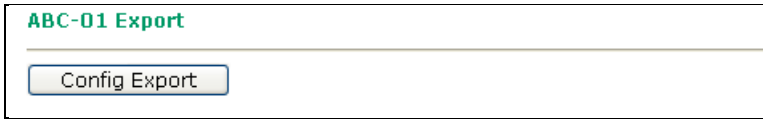


Second you also can use TFTP to back up or restore the AWK-3121-RTG's configuration with **Config Import Export**.



Third you can also back up or restore the ABC-01 (HW Rev. 1.1 support only) configuration with **Config Import Export**.





To download the configuration to the AWK:

1. Turn off the AWK.
2. Plug in the ABC-01 to the AWK's RS-232 console.
3. Turn on AWK.
4. AWK will detect ABC-01 during bootup, and download the configuration from the ABC-01 to the AWK automatically. Once the configuration downloads and if configuration format is correct, the AWK will emit three short beeps, then continue the boot up.
5. Once the AWK has booted up successfully, it will emit the normal two beeps, and the ready LED will turn to solid green.

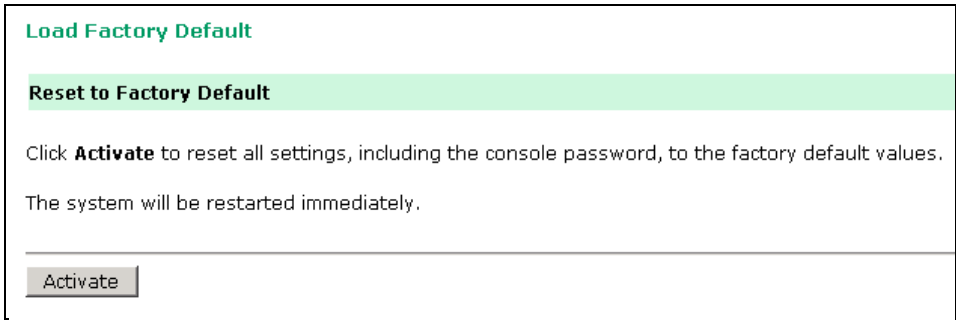
Mib Export

You can back up the AWK-3121-RTG's Mib with **Mib Export**.

click the **Mib Export** button and save the configuration file onto your local storage media. The configuration file is a text file and you can view and edit it with a general text-editing tool.

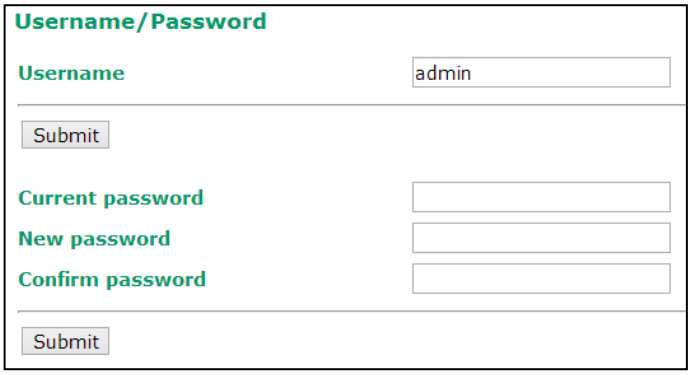
Load Factory Default

Use this function to reset the AWK-3121-RTG and roll all settings back to the factory default values. You can also reset the hardware by pressing the reset button on the top panel of the AWK-3121-RTG.



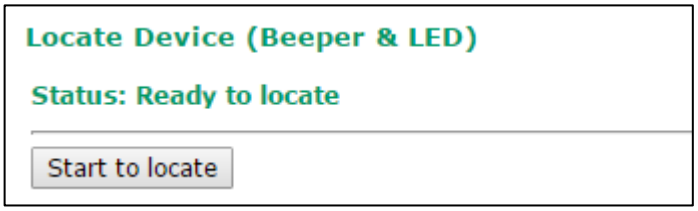
Password

You can change the administration Username and password for each of the AWK-3121-RTG's console managers by using the **Username** and **Password** function. Before you set up a new password, you must input the current password and reenter the new password for confirmation. For your security, do not use the default password ***root***, and remember to change the administration password regularly.



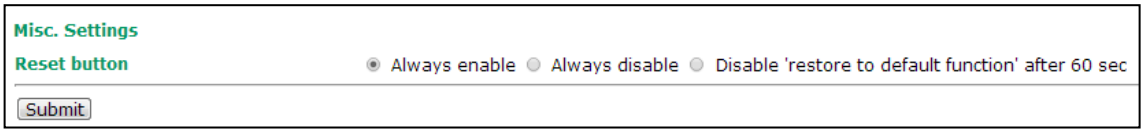
Locate Device

The AP can be identified by a beeping sound and flashing LED when clicking on the "start to locate" button. To stop the beeping, click on the "stop locating" button.



Misc. Settings

Additional settings to help you manage your AWK-3121-RTG, are available on this page.



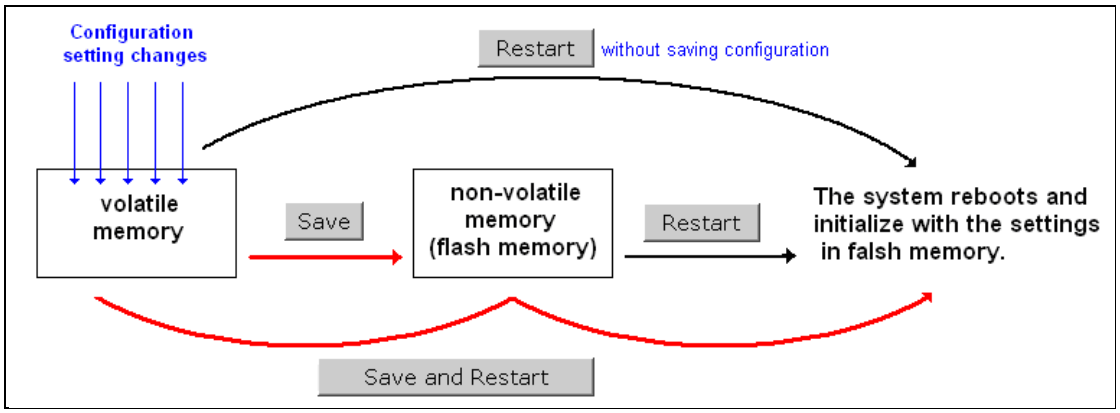
Reset button

Setting	Description	Factory Default
Always enable	The AWK-3121-RTG's Reset button works normally.	Always enable
Always disable	The AWK-3121-RTG's Reset button can't work	
Disable 'restore to default function' after 60 sec	The AWK-3121-RTG's restore to default function will be inactive 60 seconds after the AWK-3121-RTG finishes booting up.	

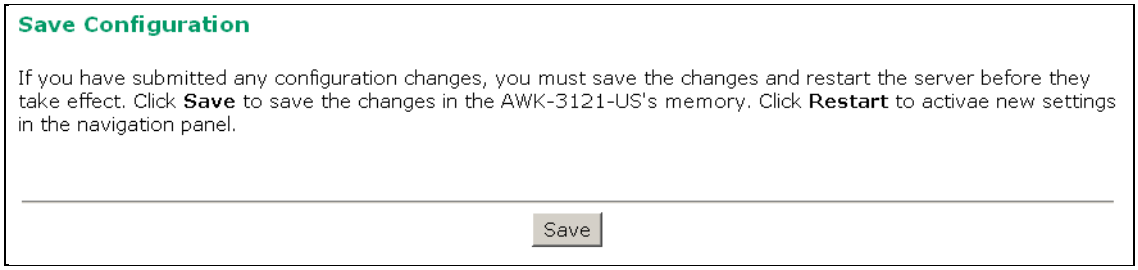
Save Configuration

The following figure shows how the AWK-3121-RTG stores the setting changes into volatile and non-volatile memory. All data stored in volatile memory will disappear when the AWK-3121-RTG is shutdown or rebooted unless they are **y**. Because the AWK-3121-RTG starts up and initializes with the settings stored in flash memory, all new changes must be saved to flash memory before restarting the AWK-3121-RTG.

This also means the new changes will not work unless you run either the **Save Configuration** function or the **Restart** function.



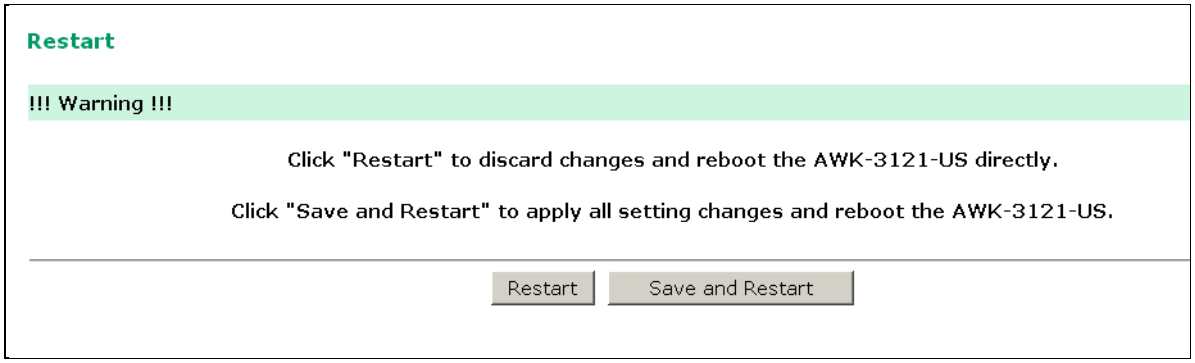
After you click on **Save Configuration** in the left menu box, the following screen will appear. Click **Save** if you wish to update the configuration settings in the flash memory at this time. Alternatively, you may choose to run other functions and put off saving the configuration until later. However, the new setting changes will remain in the non-volatile memory until you save the configurations.



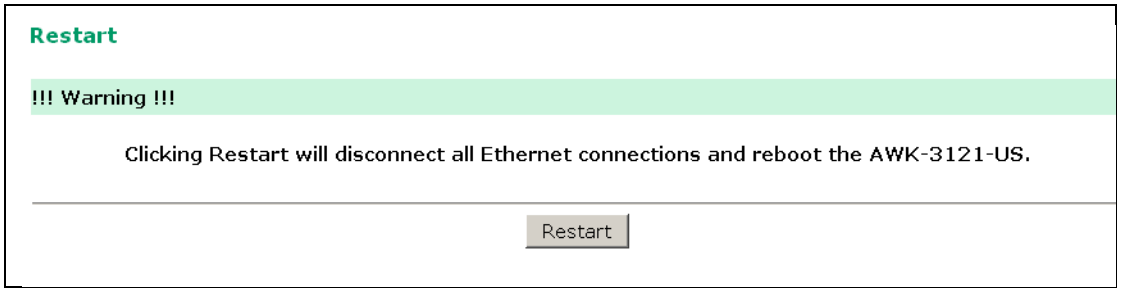
Restart

If you submitted configuration changes, you will find a blinking string in the upper right corner of the screen. After making all your changes, click the **Restart** function in the left menu box. One of two different screens will appear.

If you made changes recently but did not save, you will be given two options. Clicking the **Restart** button here will reboot the AWK-3121-RTG directly, and all setting changes will be ignored. Clicking the **Save and Restart** button will apply all setting changes and then reboot the AWK-3121-RTG.



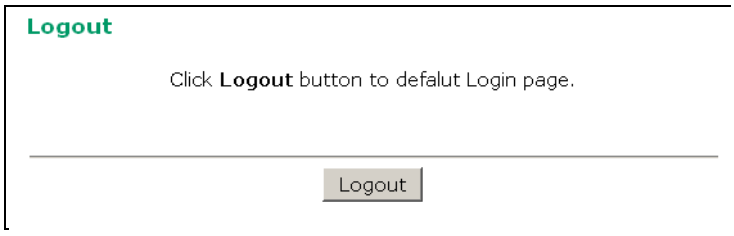
If you run the **Restart** function without changing any configurations or saving all your changes, you will see just one **Restart** button on your screen.



You will not be able to run any of the AWK-3121-RTG's functions while the system is rebooting.

Logout

Logout helps users disconnect the current HTTP or HTTPS session and go to the Login page. For security reasons, we recommend you logout before quitting the console manager.



4

Software Installation and Configuration

The following topics are covered in this chapter:

- **Overview**
- **AWK Search Utility**
  - Installing AWK Search Utility
  - Configuring AWK Search Utility

Overview

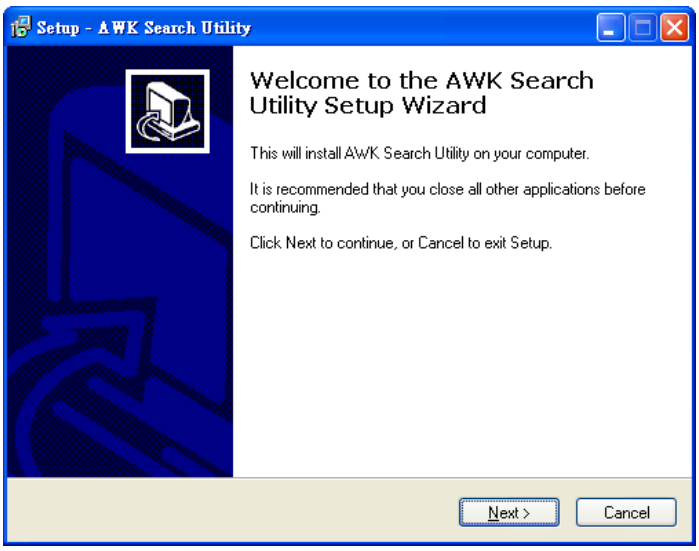
The Documentation & Software CD included with your AWK-3121-RTG is designed to make the installation and configuration procedure easy and straightforward. This auto-run CD includes AWK Search Utility (to broadcast search for all AWK's accessible over the network), the AWK-3121-RTG User's Manual, and Quick Installation Guide.

AWK Search Utility

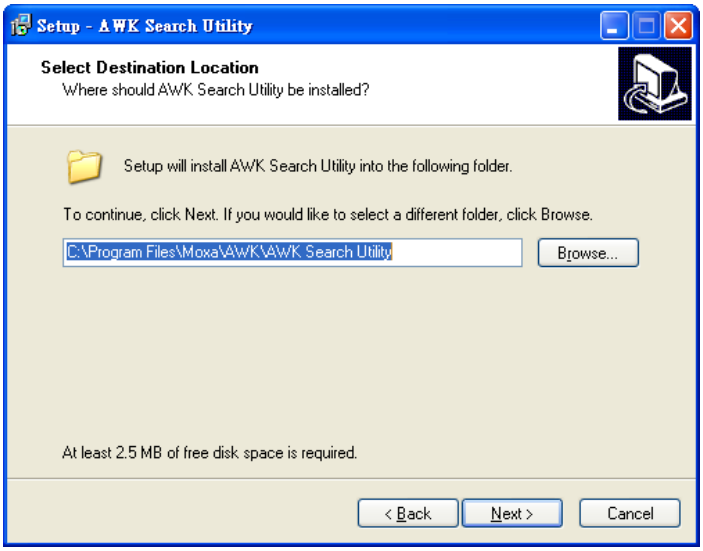
Installing AWK Search Utility

Click the **INSTALL UTILITY** button in the AWK Installation CD auto-run window to install AWK Search Utility. Once the program starts running, click **Yes** to proceed.

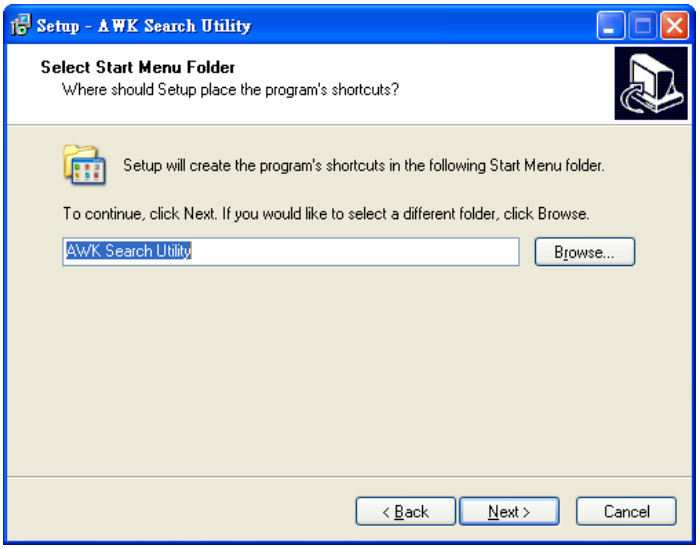
1. Click **Next** when the **Welcome** screen opens to proceed with the installation.



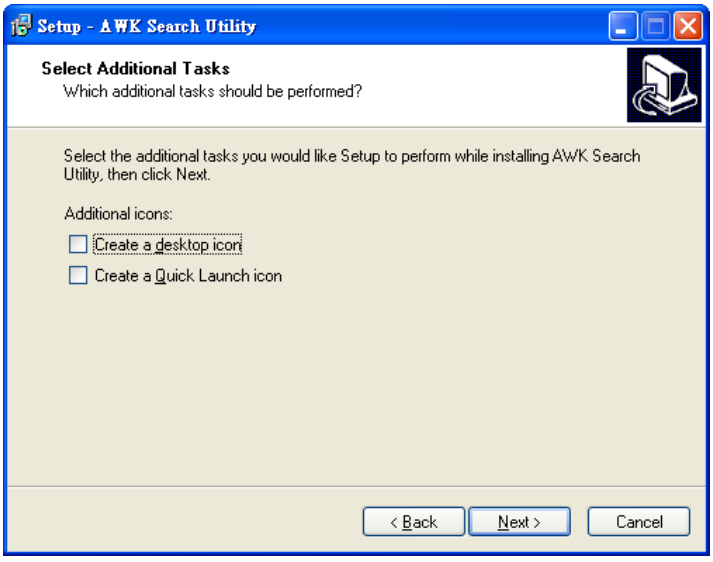
2. Click **Next** to install program files to the default directory, or click **Browse** to select an alternate location.



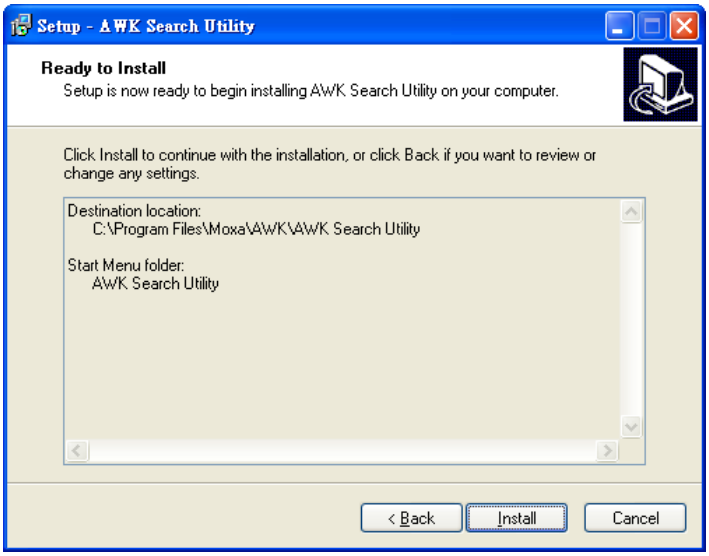
3. Click **Next** to create the program's shortcut files to the default directory, or click **Browse** to select an alternate location.



4. Click **Next** to select additional tasks.

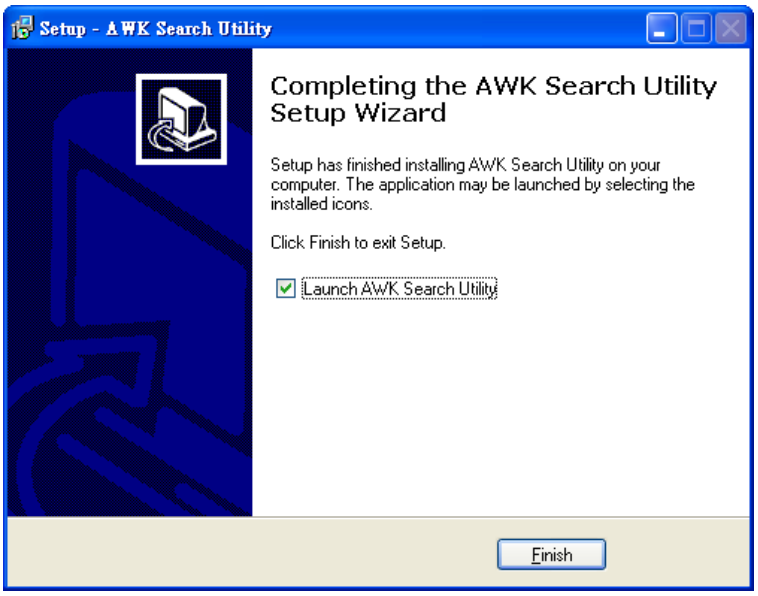


5. Click **Next** to proceed with the installation. The installer then displays a summary of the installation options.



6. Click **Install** to begin the installation. The setup window will report the progress of the installation. To change the installation settings, click **Back** and navigate to the previous screen.

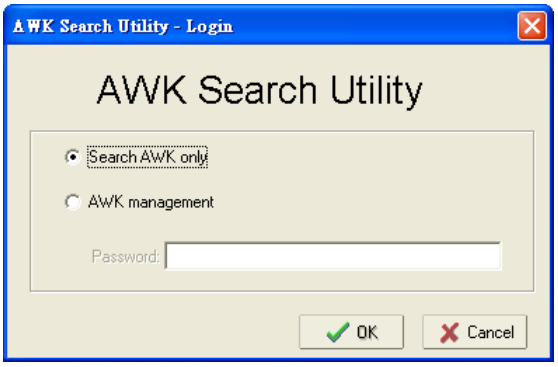
7. Click **Finish** to complete the installation of AWK Search Utility.



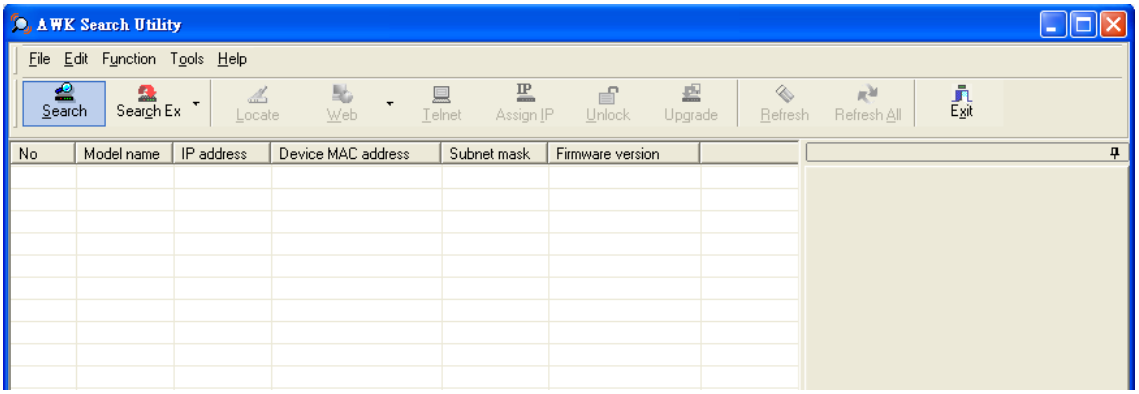
Configuring AWK Search Utility

The Broadcast Search function is used to locate all AWK-3121-RTG APs that are connected to the same LAN as your computer. After locating an AWK-3121-RTG, you will be able to change its IP address. Since the Broadcast Search function searches by TCP packet and not IP address, it doesn't matter if the AWK-3121-RTG is configured as an AP or Client. In either case, APs and Clients connected to the LAN will be located, regardless of whether or not they are part of the same subnet as the host.

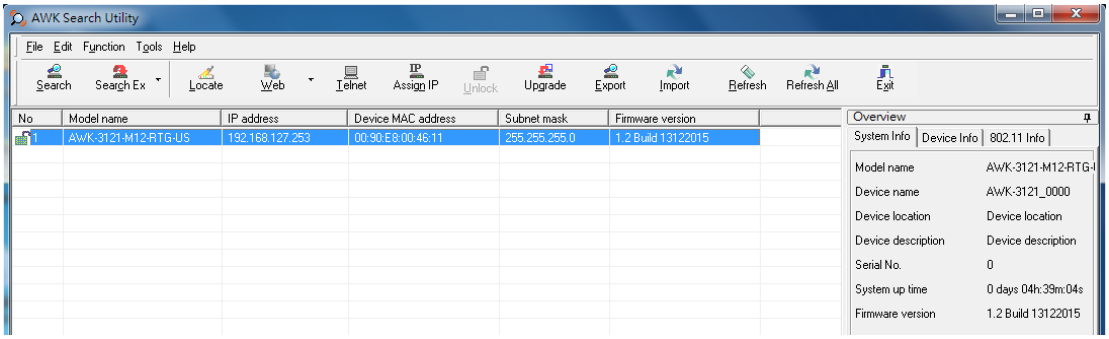
1. Start the **AWK Search Utility** program. When the Login page appears, select the "Search AWK only" option to search for AWKs and to view each AWK's configuration. Select the "AWK management" option to assign IPs, upgrade firmware, and locate devices.



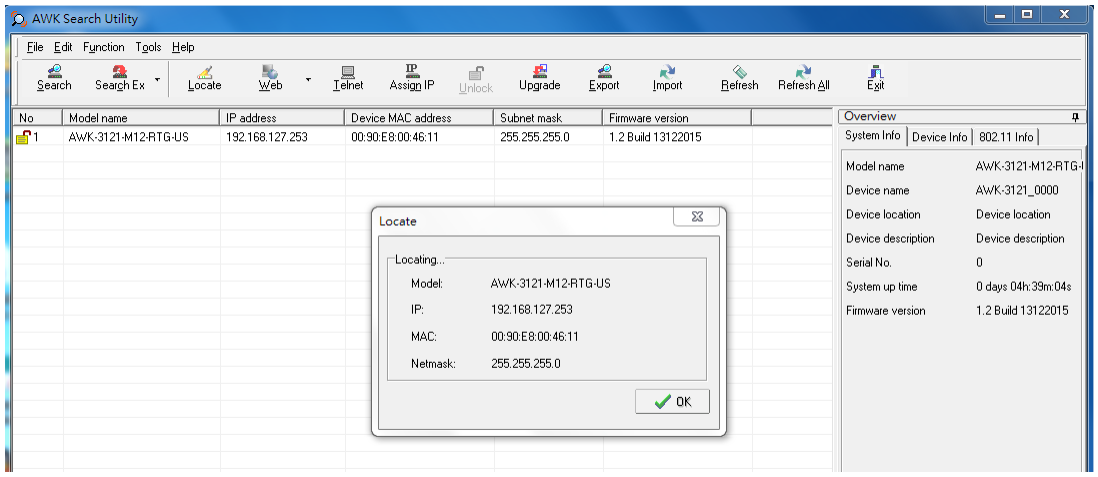
2. Open the AWK Search Utility and then click the **Search** icon.



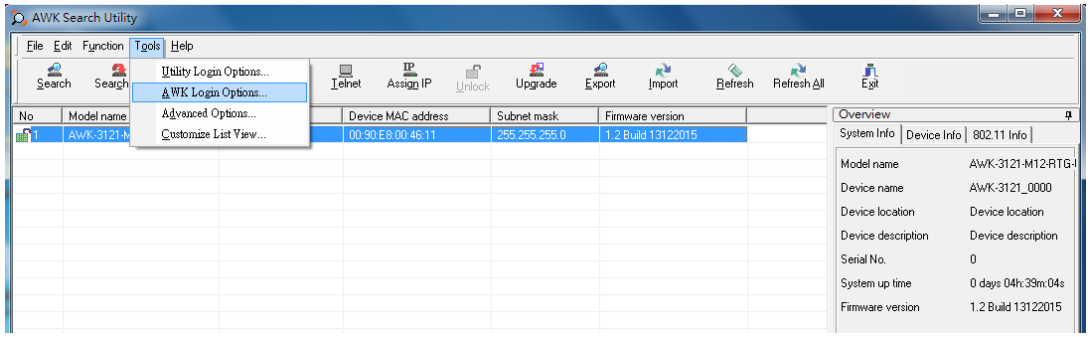
3. The "Searching" window indicates the progress of the search. When the search is complete, all AWKs that were located will be displayed in the AWK Search Utility window.



4. Click **Locate** to cause the selected device to beep.



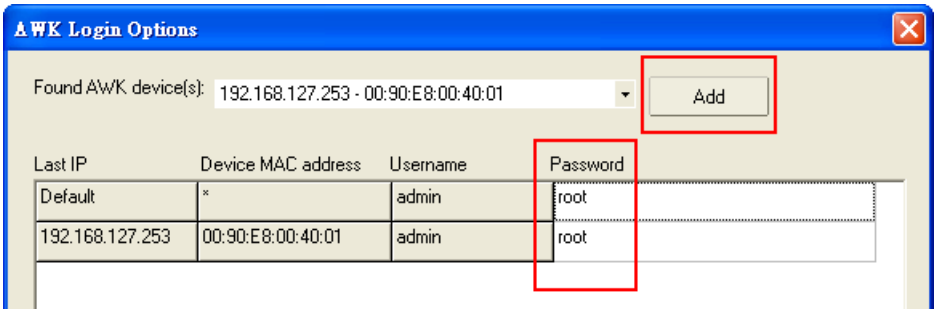
5. Make sure your AWK is **unlocked** before using the search utility's icons setting. The AWK will unlock automatically if the password is set to the default. Otherwise you must enter the new password manually.
6. Go to **Tools → AWK login Options** to manage and unlock additional AWKs.



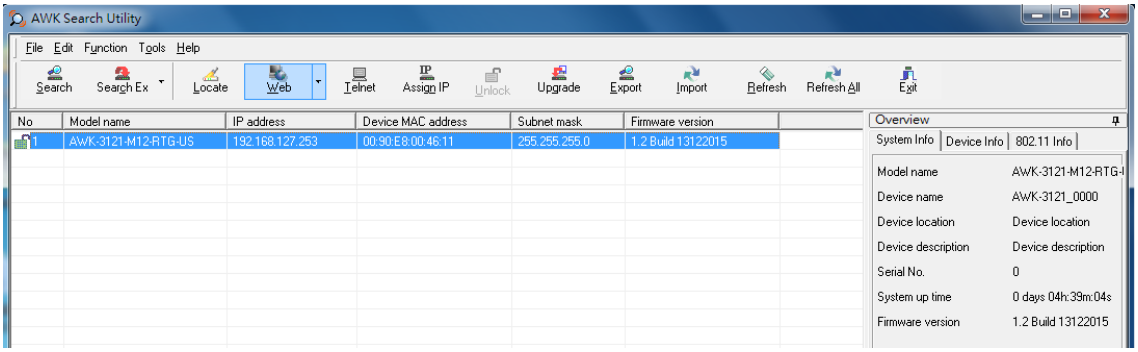
7. Use the scroll down list to select the MAC addresses of those AWKs you would like to manage, and then click **Add**. Key in the password for the AWK device and then click **OK** to save. If you return to the search page and search for the AWK again, you will find that the AWK will unlock automatically.

ATTENTION

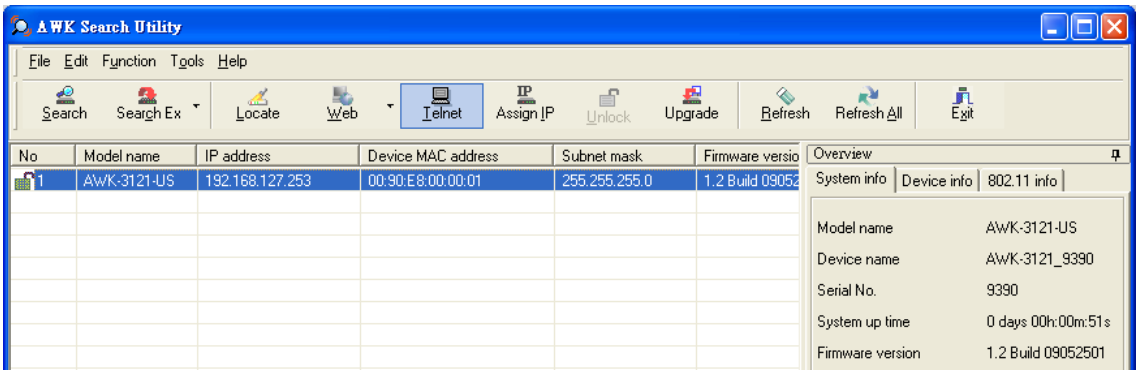
For security purposes, we suggest you can change the AWK search utility login password instead of using the default.



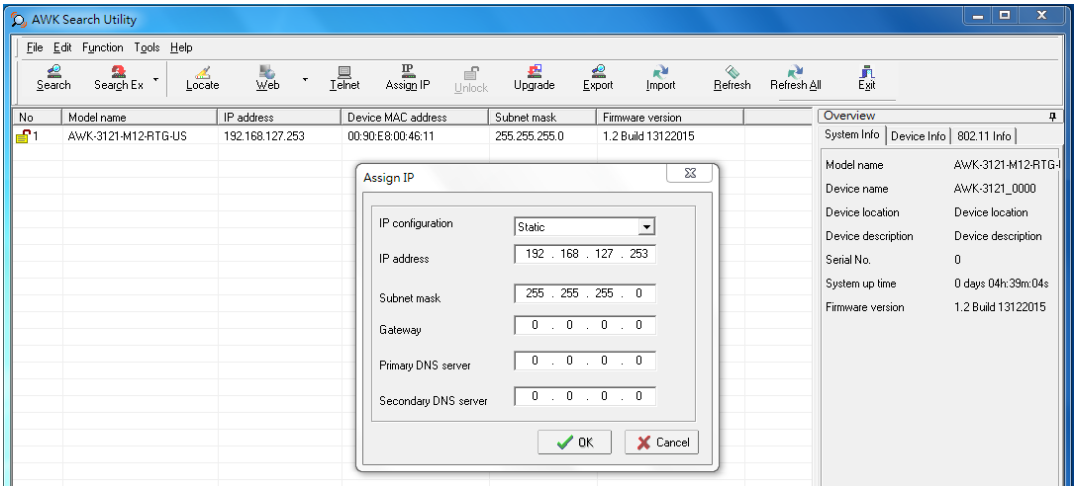
To modify the configuration of the highlighted AWK, click on the Web icon to open the web console. This will take you to the web console, where you can make all configuration changes. Refer to Chapter 3, "Using the Web Console," for information on how to use the web console.



Click on **Telnet** if you would like to use telnet to configure your AWKs.



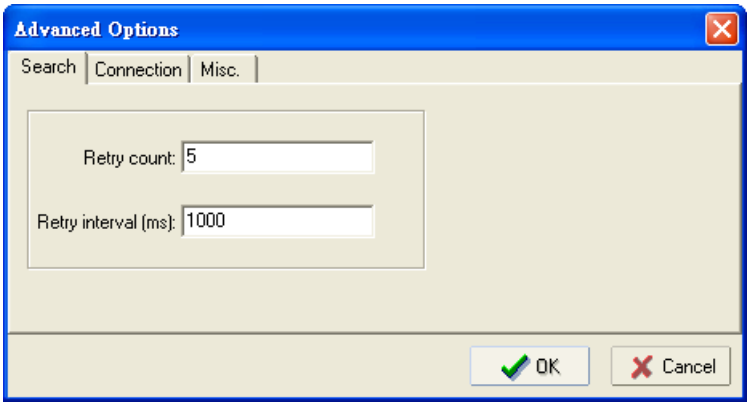
Click **Assign IP** to change the IP setting.



The three advanced options—**Search**, **Connection**, and **Miscellaneous**—are explained below:

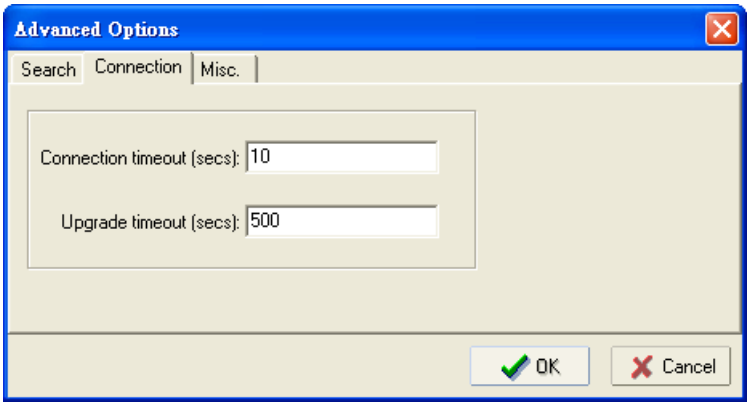
Search

- **Retry count (default=5):** Indicates how many times the search will be retried automatically.
- **Retry interval (ms):** The time lapsed between retries.



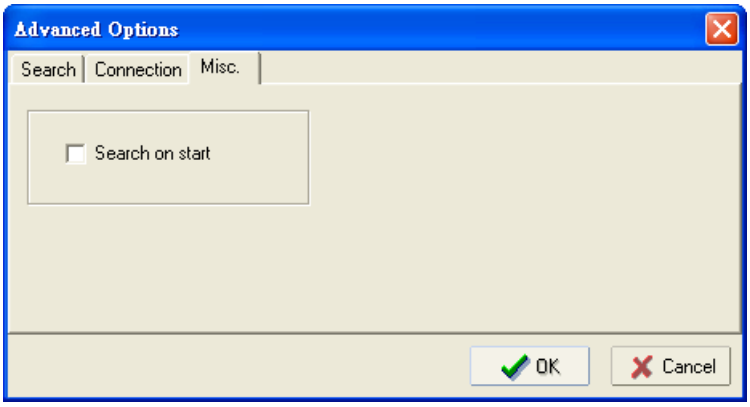
Connection

- **Connection timeout (secs):** Use this option to set the waiting time for the **Default Login**, **Locate**, **Assign IP**, **Upload Firmware**, and **Unlock** to complete.
- **Upgrade timeout (secs):** Use this option to set the waiting time for the connection to disconnect while the firmware is upgrading. Use this option to set the waiting time for the Firmware to write to flash.



Misc.

Search on start: Checkmark this box if you would like the search function to start searching for devices after you log in to the AWK search Utility.



5

Other Console Considerations

This chapter explains how to access the AWK-3121-RTG for the first time. In addition to HTTP access, there are four ways to access AWK-3121-RTG: serial console, Telnet console, SSH console, and HTTPS console. The serial console connection method, which requires using a short serial cable to connect the AWK-3121-RTG to a PC's COM port, can be used if you do not know the AWK-3121-RTG's IP address. The other consoles can be used to access the AWK-3121-RTG over an Ethernet LAN, or over the Internet.

The following topics are covered in this chapter:

- **RS-232 Console Configuration (115200, None, 8, 1, VT100)**
- **Configuration by Telnet and SSH Consoles**
- **Configuration by Web Browser with HTTPS/SSL**
- **Disabling Telnet and Browser Access**

RS-232 Console Configuration (115200, None, 8, 1, VT100)

The serial console connection method, which requires using a short serial cable to connect the AWK-3121-RTG to a PC's COM port, can be used if you do not know the AWK-3121-RTG's IP address. It is also convenient to use serial console configurations when you cannot access the AWK-3121-RTG over Ethernet LAN, such as in the case of LAN cable disconnections or broadcast storming over the LAN.

ATTENTION

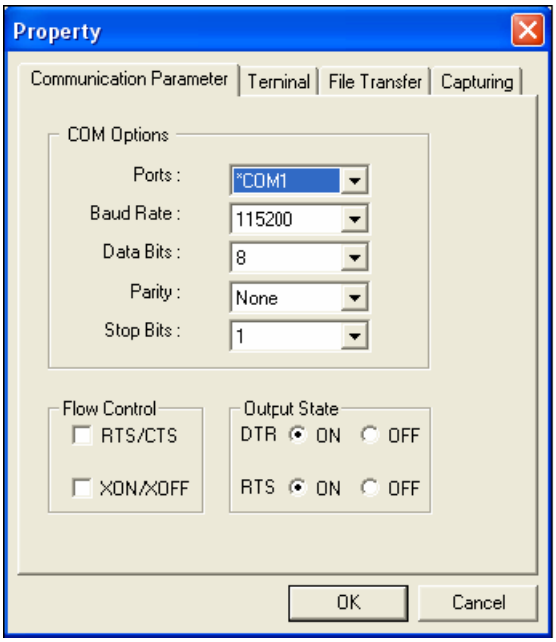
Do not use the RS-232 console manager when the AWK-3121-RTG is powered at reversed voltage (ex. -48VDC), even though reverse voltage protection is supported.
If you need to connect the RS-232 console at reversed voltage, Moxa's TCC-82 isolator is your best solution.

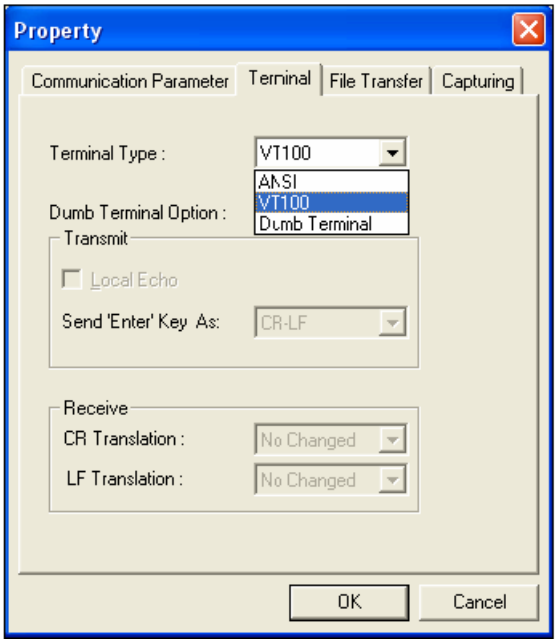
NOTE We recommend using **Moxa PComm (Lite)** Terminal Emulator, which can be downloaded free of charge from Moxa's website.

Before running PComm Terminal Emulator, use an RJ45 to DB9-F (or RJ45 to DB25-F) cable to connect the AWK-3121-RTG's RS-232 console port to your PC's COM port (generally COM1 or COM2, depending on how your system is set up). After installing PComm Terminal Emulator, take the following steps to access the RS-232 console utility.

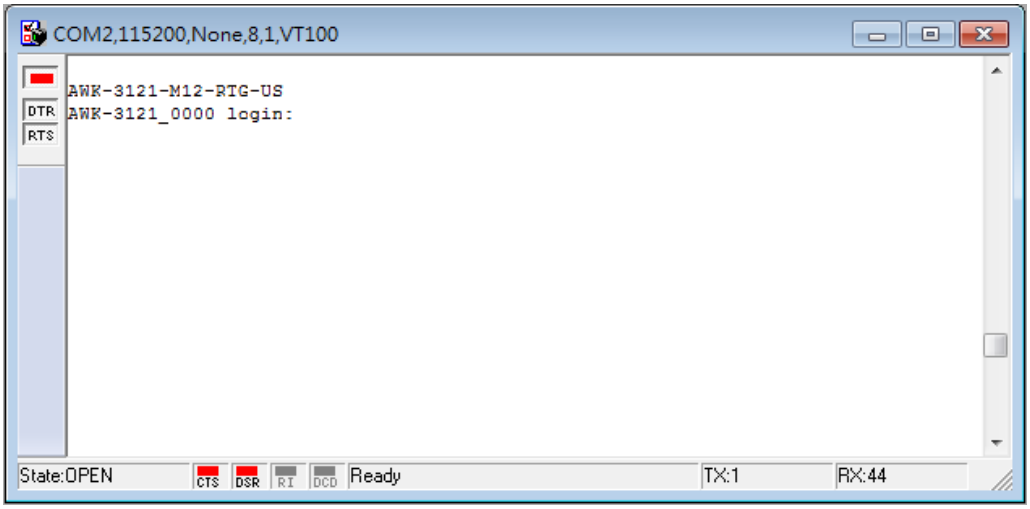
1. From the Windows desktop, open the Start menu and start **PComm Terminal Emulator** in the PComm (Lite) group.
2. Select Open under Port Manager to open a new connection.

3. The **Communication Parameter** page of the Property window opens. Select the appropriate COM port for Console Connection, **115200** for Baud Rate, **8** for Data Bits, **None** for Parity, and **1** for Stop Bits. Click on the **Terminal** tab, and select **VT100 (or ANSI)** for Terminal Type. Click on **OK** to continue.

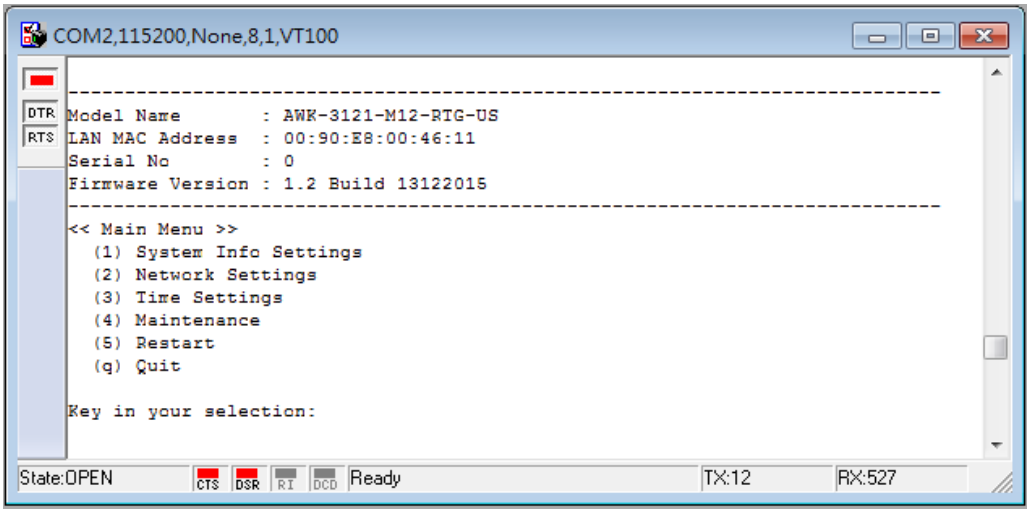




4. The Console login screen will appear. Log into the RS-232 console with the login name (default: **admin**) and password (default: **root**, if no new password is set).



5. The AWK-3121-RTG's device information and Main Menu will be displayed. Please follow the description on screen and select the administration option you wish to perform.



NOTE To modify the appearance of the PComm Terminal Emulator window, select **Edit → Font** and then choose the desired formatting options.

ATTENTION

If you unplug the RS-232 cable or trigger **DTR**, a disconnection event will be evoked to enforce logout for network security. You will need to log in again to resume operation.

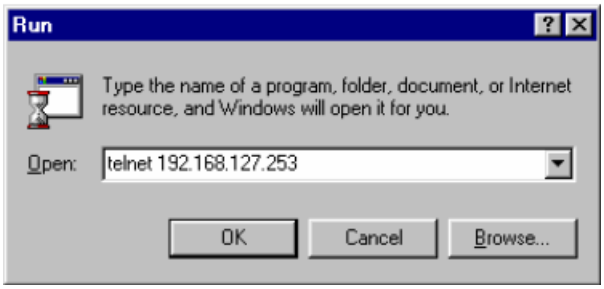
Configuration by Telnet and SSH Consoles

You may use Telnet or SSH client to access the AWK-3121-RTG and manage the console over a network. To access the AWK-3121-RTG's functions over the network from a PC host that is connected to the same LAN as the AWK-3121-RTG, you need to make sure that the PC host and the AWK-3121-RTG are on the same logical subnet. To do this, check your PC host's IP address and subnet mask.

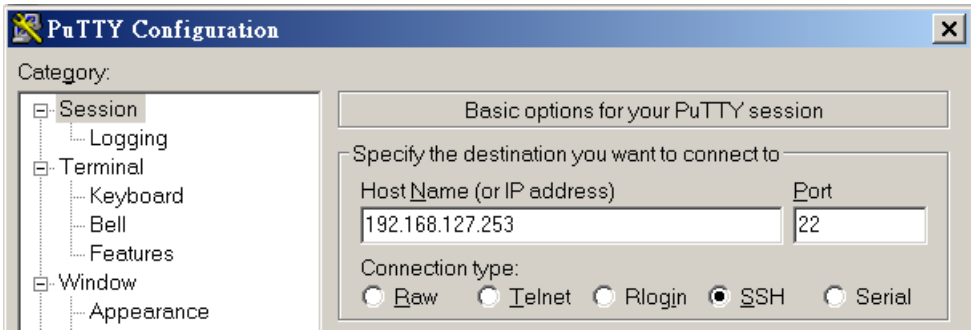
NOTE The AWK-3121-RTG's default IP address is **192.168.127.253** and the default subnet mask is **255.255.255.0** (for a Class C network). If you do not set these values properly, please check the network settings of your PC host and then change the IP address to 192.168.127.xxx and subnet mask to 255.255.255.0.

Follow the steps below to access the console utility via Telnet or SSH client.

1. From Windows Desktop, run **Start → Run**, and then use Telnet to access the AWK-3121-RTG's IP address from the Windows Run window (you may also issue the telnet command from the MS-DOS prompt).



2. When using SSH client (ex. PuTTY), please run the client program (ex. putty.exe) and then input the AWK-3121-RTG's IP address, specifying **22** for the SSH connection port.

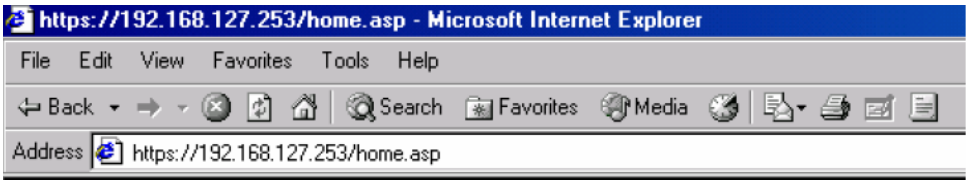


3. The Console login screen will appear. Please refer to the previous paragraph "RS-232 Console Configuration" and for login and administration.

Configuration by Web Browser with HTTPS/SSL

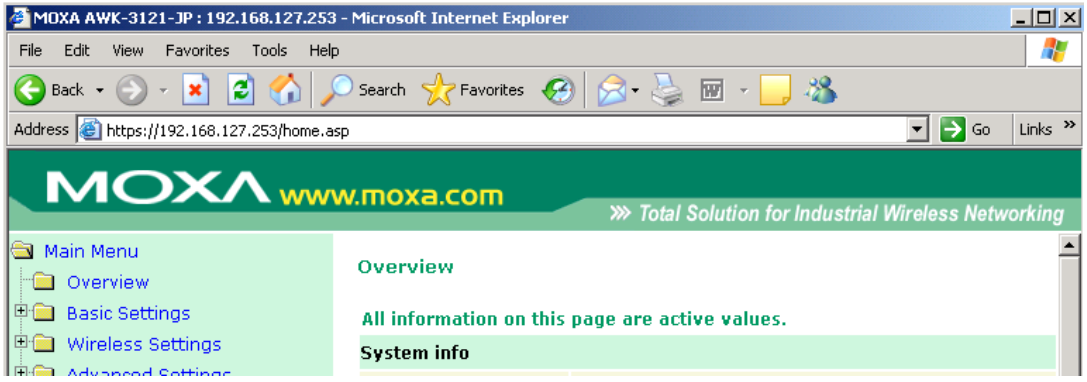
To secure your HTTP access, the AWK-3121-RTG supports HTTPS/SSL encryption for all HTTP traffic. Perform the following steps to access the AWK-3121-RTG's web browser interface via HTTPS/SSL.

1. Open your web browser and type https://<AWK-3121-RTG's IP address> in the address field. Press **Enter** to establish the connection.



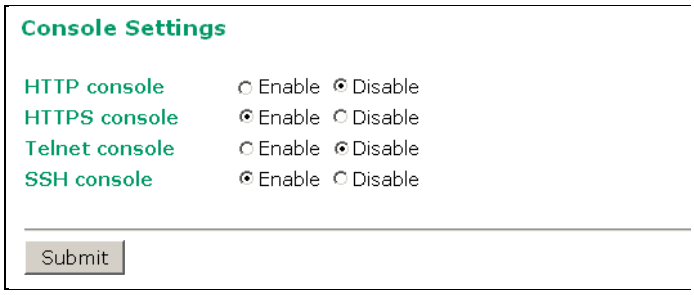
2. Warning messages will pop out to warn users that the security certificate was issued by a company they have not chosen to trust.

3. Select **Yes** to accept the certificate issued by Moxa IW and then enter the AWK-3121-RTG's web browser interface secured via HTTPS/SSL. (You can see the protocol in URL is **https**.) Then you can use the menu tree on the left side of the window to open the function pages to access each of AWK-3121-RTG's functions.



Disabling Telnet and Browser Access

If you are connecting the AWK-3121-RTG to a public network but do not intend to use its management functions over the network, then we suggest disabling both Telnet Console and Web Configuration. Please run **Maintenance → Console Settings** to disable them, as shown in the following figure.



A

References

This chapter provides more detailed information about wireless-related technologies. The information in this chapter can help you administer your AWK-3121-RTGs and plan your industrial wireless network better.

The following topics are covered in this appendix:

- **Beacon**
- **DTIM**
- **Fragment**
- **RTS Threshold**

Beacon

A beacon is a packet broadcast by the AP to keep the network synchronized. A beacon includes the wireless LAN service area, the AP address, the Broadcast destination address, a time stamp, Delivery Traffic Indicator Maps (DTIM), and the Traffic Indicator Message (TIM). Beacon Interval indicates the frequency interval of AP.

DTIM

Delivery Traffic Indication Map (DTIM) is contained in beacon frames. It is used to indicate that broadcast and multicast frames buffered by the AP will be delivered shortly. Lower settings result in more efficient networking, while preventing your PC from dropping into power-saving sleep mode. Higher settings allow your PC to enter sleep mode, thus saving power.

Fragment

A lower setting means smaller packets, which will create more packets for each transmission. If you have decreased this value and experience high packet error rates, you can increase it again, but it will likely decrease overall network performance. Only minor modifications of this value are recommended.

RTS Threshold

RTS Threshold (256-2346) – This setting determines how large a packet can be before the Access Point coordinates transmission and reception to ensure efficient communication. This value should remain at its default setting of 2,346. When you encounter inconsistent data flow, only minor modifications are recommended.

B

Supporting Information

This chapter presents additional information about this manual and product. You can also learn how to contact Moxa for technical support.

The following topics are covered in this appendix:

- **DoC (Declaration of Conformity)**
  - Federal Communication Commission Interference Statement
  - R&TTE Compliance Statement
- **Firmware Recovery**

DoC (Declaration of Conformity)

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance, (example – use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This transmitter must not be co-located or operated in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator & your body.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC 15.407(e): Within the 5.15-5.25 GHz band, U-NII devices will be restricted to indoor operations to reduce any potential for harmful interference to co-channel MSS operations.

NOTE The availability of some specific channels and / or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

R&TTE Compliance Statement

Moxa declares that the apparatus AWK-3121-RTG complies with the essential requirements and other relevant provisions of Directive 1999/5/EC.

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity (R&TTE).

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) as of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacturer must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France (with Frequency channel restrictions), Germany, Greece, Ireland, Italy, Luxembourg, Portugal, Spain, Sweden, The Netherlands, and United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states Norway and Switzerland.

EU Countries Not Intended for Use

None.

Potential Restrictive Use

France: only channels 10, 11, 12, and 13.

Firmware Recovery

When the LEDs of **FAULT**, **Signal Strength**, **CLIENT**, **BRIDGE** (no function)**,** and **WLAN** all light up simultaneously and blink at one-second interval, it means the system booting has failed. It may result from some wrong operation or uncontrollable issues, such as an unexpected shutdown during firmware update. The AWK-3121-RTG is designed to help administrators recover such damage and resume system operation rapidly. You can refer to the following instructions to recover the firmware:

Connect to the AWK-3121-RTG's ES-232 console with **115200bps and N-8-1**. You will see the following message shown on the terminal emulator every one second.

```
Section userdisk Cksum error = 0xa5feadde --> 0x658c5051
Press Ctrl-C to enter Firmware Recovering Process.....
Press Ctrl-C to enter Firmware Recovering Process.....
Press Ctrl-C to enter Firmware Recovering Process.....
Press Ctrl-C to enter Firmware Recovering Process.....
Press Ctrl-C to enter Firmware Recovering Process.....
Press Ctrl-C to enter Firmware Recovering Process.....
Press Ctrl-C to enter Firmware Recovering Process.....
Press Ctrl-C to enter Firmware Recovering Process.....
```

Press **Ctrl - C** and the following message will appear.

```
Press Ctrl-C to enter Firmware Recovering Process.....
========================================================================
IP address of AWK-3121 : 0.0.0.0
IP address of TFTP server : 0.0.0.0
========================================================================
1. Start to firmware upgrade using the above network setting immediately.
2. Change the network settings.
Enter your selection :  (1-2,enter for abort):
```

Enter **2** to change the network setting. Specify where the AWK-3121-RTG's firmware file on the TFTP server and press **y** to write the settings into flash memory.

```
==========================================================================
IP address of AWK-3121 : 0.0.0.0
IP address of TFTP server : 0.0.0.0
==========================================================================
1. Start to firmware upgrade using the above network setting immediately.
2. Change the network settings.
Enter your selection :  (1-2,enter for abort): 2

IP address of AWK-3121 : 192.168.1.2
IP address of TFTP server : 192.168.1.1
Update RedBoot non-volatile configuration - continue (y/n)? y
```

AWK-3121-RTG restarts, and the "Press Ctrl-C to enter Firmware Recovery Process…" message will reappear. Press **Ctrl-C** to enter the menu and select **1** to start the firmware upgrade process.

```
Press Ctrl-C to enter Firmware Recoverying Process.......
==========================================================================
IP address of AWK-3121 : 192.168.1.2
IP address of TFTP server : 192.168.1.1
==========================================================================
1. Start to firmware upgrade using the above network setting immediately.
2. Change the network settings.
Enter your selection :  (1-2,enter for abort): 1
```

Select **0** in the sub-menu to load the firmware image via LAN, and then enter the file name of the firmware to start the firmware recovery.

```
==========================================================================
Load method select :
0. Load from LAN
1. Load from serial with Xmodem
q. Abort select.
==========================================================================
Please select item : 0
Please input load image name..
Default file name : AWK-3121.rom
User Input file name : AWK-3121_1.0.rom
```